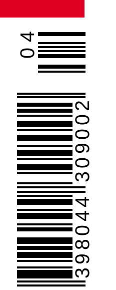
DM 9,–/SFR 9,–/ÖS 68,– B 30671
4/2000

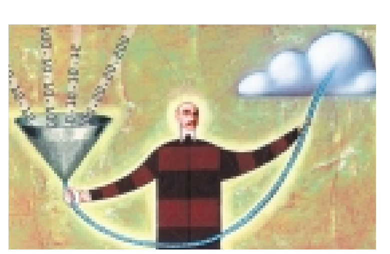
Das Original ➤ NT Magazin

Windows® 2000 magazin



Marktübersicht: ISDN-Software für NT und Windows 2000

Praktisch für kleine Netze:



Komfortabel und preiswert ins Internet mit Windows 2000

CeBIT 2000 Nachlese



- Die wichtigsten Trends
- Die interessantesten Produkte





- Ratgeber: Die richtige Firewall auswählen
- Marktübersicht: Internet Solution Provider
- Windows-Programme im Internet publizieren
- Mobile Banking per Handy und WAP

INTERNET Sicherheit



Windows 2000 Aktuell

- Im Test: •Suresync Real-Time •Remote Recover •Aelita Enterprise Suite
- Aktuell: Windows-2000-Launch – zwischen Party und Gerichtssaal
- Umfrage: PC-Hersteller setzen auf Windows 2000

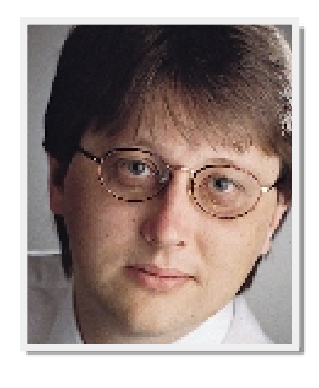
Know-how: NT-Domänen nach Windows 2000 migrieren

Grundlagenwissen: NT-Domänen-Controller

JETZT NEU! Für NT- und Windows-2000-Profis



www.win2000mag.de



Willkommen beim Windows 2000 Magazin

Gehören Sie zu den langjährigen Lesern des NT Magazins oder halten Sie die Zeitschrift – angezogen durch den neuen Titel „Windows 2000 Magazin" – zum ersten Mal in Händen? Auf jeden Fall heißen wir Sie herzlich willkommen. Wenn Sie Windows NT oder Windows 2000 installieren, konfigurieren, warten und supporten müssen, sind Sie beim Windows 2000 Magazin ebenso richtig wie wenn Sie als Power-User Ihr System optimieren möchten oder als Netzwerkadministrator den sicheren Einsatz der Server zu gewährleisten haben.

Unser Ziel ist es, Sie aktuell über alle wichtigen Trends rund um Windows NT und den NT-Nachfolger Windows 2000 zu informieren. Sie finden so in der Rubrik „Markt" nicht nur Berichte über Messen und Kongresse, sondern auch Interviews, einen Veranstaltungskalender sowie Ergebnisse von Umfragen.

In der Rubrik „Wissen" geht es ans Eingemachte. Renommierte NT-Experten aus den USA und Deutschland nehmen neue Technologien unter die Lupe und erklären die Interna von Betriebssystem und Anwendungen.

Die Rubrik „Toolkit" – also Werkzeugkasten – ist in zweierlei Hinsicht zu verstehen. Einerseits stellen wir Ihnen hier nützliche Werkzeuge, beispielsweise aus den Resource-Kits oder aus der Free- und Shareware-Szene vor. Zum Handwerkszeug gehört aber auch das notwendige Praxis-Know-how. Dies vermitteln wir in zahlreichen Workshops, Tipps & Tricks sowie Antworten auf Hotline-Probleme.

Um Produkte geht es in der Rubrik „Lab-Report". Hier finden Sie unabhängige Berichte aus unserem Testlabor. Wir stellen Ihnen aber auch interessante Neuentwicklungen vor. Schließlich finden Sie in jeder Ausgabe eine ausführliche Marktübersicht zu einem wichtigen Produktbereich.

Jede Ausgabe enthält einen „Fokus", in dem mehrere Artikel zu einem „heißen" Thema zusammengestellt sind. In diesem Monat geht es um sichere Internet-Anwendungen. Ergänzend dazu finden Sie eine Übersicht mit Internet Solution-Providern, die über Know-how bei der Erstellung oder dem Hosting von E-Business-Anwendungen verfügen.

Wir in der Redaktion sind natürlich gespannt, wie Ihnen das Windows 2000 Magazin gefällt. Schreiben Sie uns Ihre Meinung, und auch, was Sie in Zukunft im Windows 2000 Magazin lesen möchten. Am besten per E-Mail an Redaktion@win2000mag.de.

Ihr

Frank-Martin Binder

INHALT

4/2000

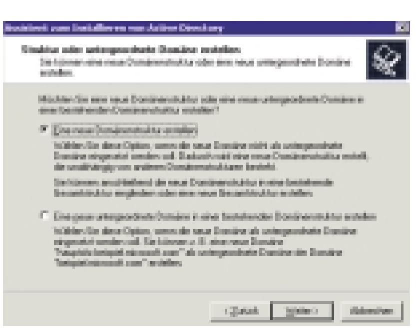
Ab Seite





Internet-anbindung mit Windows 2000 und NAT

Einen einzelnen Rechner ans Internet anzubinden, ist kein Problem. Erheblich anspruchsvoller wird es, wenn ein kleines Netzwerk über eine günstige Wählleitung mit dem weltweiten Netz kommunizieren soll. Mit der integrierten Network Address Translation (NAT) hat Windows 2000 das richtige Werkzeug schon an Bord.



Ab Seite 42

Keine Angst vorm Windows-2000-Upgrade

Ein Windows-NT-Netzwerk ist von seinen Domänen-Controllern abhängig. Sie bilden das Fundament, auf dem alle Dienste aufsetzen. Deshalb scheuen sich viele Administratoren, diese kritischen Maschinen aufzurüsten. Wir sagen Ihnen, wie Sie Ihre Domänen-Controller sicher auf Windows 2000 und Active Directory migrieren.

Ab Seite 74

Windows-Anwendungen sicher über das Internet publizieren

Mit dem Windows NT Terminal Server und Citrix Metaframe lassen sich Windows-Anwendungen nicht nur im internen Netz von fast jedem Client aus nutzen. Der geringe Bandbreitenbedarf macht auch die Nutzung über das Internet attraktiv. Doch Vorsicht! Allzuleicht reißt man große Löcher in die Firewall.

DIALOG

MARKT

WISSEN

TOOLKIT

Ab Seite 79

Die Auswahl der richtigen Firewall

Fast täglich findet man in den Medien Horrormeldungen über Einbrüche in Computernetze, Datendiebstahl und Virenangriffe. Eine Möglichkeit, sich gegen solche Gefahren zu schützen, sind Firewalls. Doch wie müssen diese aufgebaut sein, um allen lauernden Gefahren entgegenzutreten?

Ab Seite 10 + 59



CeBIT-Nachlese: Trends und Produkte

Windows 2000 war eines der Top-Themen auf der CeBIT in Hannover. Wir haben die wichtigsten Trends aufgespürt und die interessantesten Produkte für NT und Windows 2000 für Sie zusammengestellt.



LAB-REPORT

FOKUS

RUBRIKEN



Windows 2000 Glossar
Mit Windows 2000 kommen nicht nur zahlreiche neue Technologien auf den Anwender zu, sondern auch jede Menge neuer Begriffe und Akronyme. Das auf dem Titel aufgeklebte Glossar hilft Ihnen durch den Begriffe-Dschungel.

Wenn es schon jemand vor Ihnen gebrauchen konnte, kein Problem: Schreiben Sie an Windows 2000 Magazin und legen Sie einen mit DM 2,20 frankierten und an Sie adressierten C6-Rückumschlag bei. Wir schicken Ihnen das Glossar dann umgehend und kostenlos zu.

Unsere Anschrift:
AWi Vertriebsservice
Herzog-Otto-Str. 42
83308 Trostberg

Kontaktbörse: Usergroups zu Windows NT und Windows 2000

NT-Anwendergruppe
c/0 AddOn Systemhaus GmbH
Sindelfinger Allee 25
71034 Böblingen
Tel.: 0 70 31/71 77-55
Fax: 0 70 31/71 77-10
Web: http://www.nt-ag.de

SAP R/3 NT User Group e.V.
c/o PC & PR GmbH
Kölner Straße 51
53894 Mechernich-Kommern
Telefon: 0 24 43/60 89
Fax: 0 24 43/51 02
E-Mail: KlausHopp@pcpr.de
Web: http://www.r3-nt-user-group.de

NT User Group
c/o IIR Deutschland GmbH
Lyoner Str. 26
60528 Frankfurt/M.
Tel.: 069/5 06 04-159
Fax: 069/5 06 04-199
E-Mail: japrdey@iir.de

Windows User Group Österreich
Marinelligasse 5/2
A-1020 Wien
Tel.: 02 22/2 16 31 50-13
Fax: 02 22/2 16 31 76
E-Mail:
Josef.Reichholf@reichholf.at
Web: http://www.wug.or.at

Schreiben Sie uns, wenn Ihre Usergroup oder Anwendergruppe in dieser Liste vertreten sein soll. Dabei kommt es nicht darauf an, ob Sie eine großartige Organisation haben oder wie viele Mitglieder Ihre Usergroup hat. Sie sollten allerdings offen für neue Mitglieder sein und natürlich etwas mit Windows NT und Windows 2000 zu tun haben. Wir veröffentlichen auch gerne Hinweise auf Ihre Veranstaltungen. Sie finden unsere Adresse im nebenstehenden Kasten.

Aufruf zum Dialog

Ab der nächsten Ausgabe des Windows 2000 Magazins wollen wir Ihnen an dieser Stelle ein Forum geben. Natürlich interessiert uns ganz besonders, wie Ihnen das erneuerte NT Magazin/Windows 2000 Magazin gefällt. Haben wir Ihren Geschmack getroffen? Passt die Mischung zwischen Windows-NT- und Windows-2000-Themen oder kommt Ihnen etwas zu kurz? Wir freuen uns darauf, von Ihnen reichlich Anregungen, Kritik und Kommentare zu bekommen.

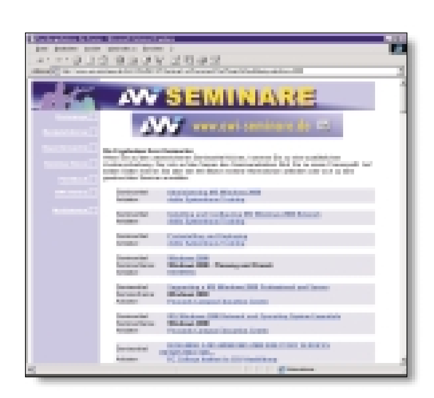
Außerdem werden wir voraussichtlich noch im April ein Diskussionsforum auf unserer Website www.win2000mag.de eröffnen. Hier haben Sie dann Gelegenheit, Meinungen mit anderen NT/Windows-2000-Profis auszutauschen oder den anderen mit Ihrem Know-how bei Problemen weiterzuhelfen (hoffentlich funktioniert das dann auch umgekehrt <g>). Also schauen Sie regelmäßig vorbei und diskutieren Sie mit. Über Anregungen, ob und wenn ja wie wir das Forum gliedern sollen, sind wir übrigens dankbar.

Ihre Redaktion Windows 2000 Magazin

So erreichen Sie das Windows 2000 Magazin

Redaktion Windows 2000 Magazin
Bretonischer Ring 13
D-85630 Grasbrunn
Fax: 089/45616-300
E-Mail: Redaktion@win2000mag.de
WWW: http://www.win2000mag.de

Web-Tipp: Online-Seminarführer



Ständig auf dem Laufenden zu bleiben und neue Qualifikationen zu erwerben, ist ein absolutes Muss in der schnellebigen EDV-Branche. Gerade, wenn ein einschneidender Release-Wechsel wie von Windows NT auf Windows 2000 ansteht, muss das eigene Know-how wieder auf den aktuellen Stand gebracht werden.

Hier hilft der AWi Online-Seminarführer (http://www.awi-seminare.de), aus der Fülle des Angebots die richtigen Seminare und Schulungen herauszufiltern. Unter den tausenden von Seminarangeboten finden sich auch eine große Menge von Schulungen rund um Windows 2000. Wer sich beispielsweise zum Microsoft Certified Systems Engineer (MCSE) zertifizieren möchte, kann sich im Online-Seminarführer die maßgeschneiderte Ausbildung heraussuchen.

Zu jedem der in der Seminardatenbank enthaltenen Anbieter finden Interessenten ein ausführliches Firmenprofil mit einer Beschreibung des Seminarprogramms, Informationen über Herstellerzertifizierungen und besondere Qualifikationen. Über ein Infoformular kann man bequem direkten Kontakt mit den Anbietern aufnehmen und weitere Informationen anfordern. Zu jedem Seminar lassen sich nicht nur eine ausführliche Kursbeschreibung, sondern auch weitergehende Informationen wie erforderliche Vorkenntnisse, Zielgruppen sowie weitere Materialien abrufen. Schließlich erhält der Interessent eine Liste aller angebotenen Seminartermine, inklusive Zeit, Ort und Dauer des Seminars sowie – nicht zu vergessen – den Preis. Wer zeitlich flexibel ist, findet zudem in einer Restplatzbörse interessante Schulungsangebote zum Schnäppchenpreis.

Erschlossen wird das Angebot durch eine Volltextsuche sowie verschiedene Listen, in denen die Seminare nach Zielgruppe, Betriebssystem und anderen Kriterien sortiert sind. Wer hier nicht fündig wird, kann über die „Expertensuche“ ausgefeilte Suchabfragen formulieren.

(fbi)



Die wichtigsten Trends von der CeBIT 2000

Windows auf dem Weg ins E-Business

750.000 Besucher und 7802 Aussteller haben die Show der Superlative wieder einmal überstanden. Sie erlebten eine Branche, die vor Zuversicht strotzt, schneller denn je neue Produkte, Technologien und Geschäftsmodelle entwirft und einen Windows-2000-Launch, der nur wenig Aufregung hervorrief.

Die CeBIT war in diesem Jahr wieder einmal gigantisch: 750.000 Besucher, davon 137.000 aus dem Ausland, 7802 Aussteller auf 415.000 Quadratmetern Fläche. Allein am Montag, dem besucherstärksten Tag, bevölkerten über 130.000 Besucher das Messegelände. Viel wichtiger als diese beeindruckenden Zahlen war jedoch die Stimmung in Hannover. Es war deutlich zu spüren, dass in der gesamten EDV-Welt eine enorme Aufbruchstimmung herrscht. Man hatte das Gefühl, als sei ein Knoten geplatzt. Nach all den defensiven Jahren, in denen man sich vorwiegend gegen die Jahr-2000-Gefahren wappnete, war wieder Nach-vorne-Denken angesagt.



Und alle dachten in dieselbe Richtung: Welche Chancen und Möglichkeiten bietet das Internet für das eigene Geschäft. Natürlich denkt man bei E-Business zuerst an Shop-Systeme, Bezahlen im Internet etc. In diesem klassischen E-Commerce gab es natürlich massenhaft Anwendungen und Lösungen zu sehen. Die wirklich spannenden Neuentwicklungen finden sich derzeit jedoch im so genannten „Business-to-Business“-Bereich. Ganz heiß gehandelt werden so genannte Business-to-Business-Marktplätze. Diese sollen die Art und Weise wie Firmen miteinander Handel treiben, revolutionieren. Beispielsweise eröffnen sich durch Optimierung von Bestellprozessen und die effiziente Lieferanteneinbindung enorme Potentiale zu Kosteneinsparung. Außerdem bietet sich den Unternehmen die Chance, ganz neue Marktplätze und Vertriebswege aufzubauen.

Unter den Firmen, die die Infrastruktur und die Lösungen für diese Marktplätze der Zukunft liefern wollen, finden sich sowohl etablierte Player wie beispielsweise SAP mit ihrem Internet-Business-Portal mysap.com, aber auch Newcomer wie die amerikanische Firma Commerce One. Diese stellte auf der CeBIT Partnerschaften mit Compaq und der deutschen Telekom vor und ist insbesondere deswegen für uns interessant, weil sie ein Beispiel dafür darstellt, wie sehr sich mittlerweile auch die Microsoft-Technologie dem Internet-Business geöffnet hat. Ihre Lösungen Buysite und Marketsite basieren nämlich auf Windows NT und Windows 2000. Ein anderes interessantes Beispiel für Internet-Anwendungen auf Basis von Microsoft-Technologie wurde von der deutschen Firma Media Artist vorgestellt. Sie präsentierte auf der CeBIT ihr Content-Management-System Internews 2000 auf Basis von Windows 2000 Advanced Server und SQL Server 7.

Schließlich eröffnet das Internet die Möglichkeit, gänzlich neue Wege beim Einsatz von Anwendungslösungen zu gehen. An die Stelle kompletter Software-Pakete, die vom Kunden gekauft und auf eigener Hardware mit eigenem Personal eingesetzt werden, tritt die Idee, Anwendungen einfach nach Bedarf zu mieten. Die Notwendigkeit, eigenes Fachpersonal für die Hardware- und Software-Wartung einzustellen, entfällt ebenso wie Einstiegshürden durch allzu hohe Anschaffungskosten. Neue Märkte über dieses so genannte Application Service Providing (ASP) will beispielsweise Ixos erschliessen, Spezialist für Dokumentenmanagement und -archivierung im SAP-R/3-Umfeld. Große Chancen rechnen sich auch Spezialisten wie das WTS-Testcenter aus, die über den Windows-Terminal-Server Office-Applikationen und andere Windows-Anwendungen im Internet publizieren wollen. Aber auch die Microsoft-Konkurrenz wittert angesichts des ASP-Booms Morgenluft: Oracle sieht sich mit seinen komplett über Browser verfügbaren Applications auf dem richtigen Pfad. Zusammen mit Compaq und dem Internet-Solution-Provider Cable & Wireless ECRC stellte Oracle unter dem Namen „Easy ASP“ ein Basispaket, bestehend aus Hardware, Betriebssystem, Datenbank, Web-Server-Anwendungen und Hosting-Komponenten vor.

> **TIP**
> Auf unserer Web-Site www.win2000mag.de finden Sie Links zu den Websites aller genannten Firmen. Außerdem können Sie mit unserem Web-Kennzifferndienst unter www.win2000mag.de/info bequem weitere Informationen bei den Firmen anfordern.

Aber da war doch noch etwas außer dem Internet. Ja richtig, Windows 2000 hatte auf der CeBIT seine Premiere. Doch der Deutschland-Launch ging im allgemeinen Messerummel ziemlich unter. Es war deutlich zu spüren, dass Microsoft das mei-



Veranstaltungskalender

Datum	Veranstaltung	Ort
März		
27.3. bis 29.3.2000	**Windows 2000 Deployment Conference** www.microsoft.com/europe/win2000dc/	Genf, Schweiz Tel.: 089-31760
28.3. bis 29.3.2000	**3. IT-Kongress Windows 2000** www.microsoft.de/isapi/germany/technet/eventkalender.asp	Neuss, Deutschland Tel.: 089-31760
April		
4.4. bis 5.4.2000	**Windows DNA 2000 Readiness Conference** www.microsoft.com/europe/dnaready/welcome.htm	Amsterdam, Niederlande Tel.: 089-31760
4.4.2000	**Cobol on Tour** www.cobolinfo.de	Kassel, Deutschland Tel.: 07141-936925
5.4. bis 7.4.2000	**SQM 2000 & ICSTEST – Int. Konferenz zum Software-Test** www.icstest.com	Bonn, Deutschland Tel.: 02203-91540
6.4.2000	**Cobol on Tour** www.cobolinfo.de	Stuttgart, Deutschland Tel.: 07141-936925
10.4. bis 12.4.2000	**Deutscher Multimedia Kongress** www.dmmk.de	Stuttgart, Deutschland Tel.: 0711-1222862
25.4. bis 27.4.2000	**WinHEC (Windows Hardware Engineering Conference) 2000** www.microsoft.com/winhec/	New Orleans, USA Tel.: 089-31760
Mai		
2.5. bis 4.5.2000	**Infobase** www.infobase.de	Frankfurt am Main, Deutschland Tel.: 069-75756866
8.5. bis 9.5.2000	**Infotage eShopsysteme** www.management-forum.de	Frankfurt am Main, Deutschland Tel.: 08151-27190
15.5. bis 16.5.2000	**4. Windows NT/Windows 2000 Forum** www.debis-training.de	Frankfurt am Main, Deutschland Tel.: 069-82999755
16.5. bis 18.5.2000	**CT NETZE 2000** www.ctnetze.de	Wiesbaden, Deutschland Tel.: 089-88919208
23.5. bis 25.5.2000	**Internet World** www.internetworld-messe.de	Berlin, Deutschland Tel.: 089/741 17-270
24.5.2000	**CAD-Forum** www.cadforum.de	Stuttgart, Deutschland Tel.: 0234-5000146
Juni		
4.6. bis 7.6.2000	**mecon – Fachkongress für digitale Medienproduktion** www.mecon.de	Köln Messe, Deutschland Tel.: 0221-916550
5.6. bis 8.6.2000	**Microsoft Tech Ed 2000** www.microsoft.com/events/teched/default.asp	Orlando, USA Tel.: 089-31760
6.6. bis 8.6.2000	**XML ONE Europe** www.xmlconference.com	Frankfurt am Main, Deutschland Tel.: 02202-93720
Juli		
4.7. bis 7.7.2000	**Microsoft Tech Ed 2000 Europe** www.microsoft.com/europe/teched/	Amsterdam, Niederlande Tel.: 089-31760

Alle Angaben ohne Gewähr.

ste Pulver bereits eine Woche zuvor beim weltweiten Launch in San Francisco verschossen hatte. Dennoch gab es viel zum Thema Windows 2000 zu hören. Kaum eine Pressekonferenz – gleich, ob bei Hardware- oder Software-Herstellern – verging ohne ein Committment zu Windows 2000. Nicht nur am Microsoft-Stand wurde Windows 2000 prominent präsentiert, sondern auch an Messeständen, wo man das nicht ohne weiteres erwartet hätte. Beispielsweise wimmelte es am Stand des ERP-Herstellers Damgaard geradezu vor Windows-2000-Ballons. Bei vielen Herstellern bekam man allerdings zu hören, dass die Entwicklung noch nicht abgeschlossen sei oder man sich noch in der Testphase befinde. Ein Fazit „CeBIT 2000 im Zeichen von Windows 2000“, wie eine Microsoft-Pressemitteilung titelte, wäre doch ein wenig übertrieben.

Der Gerechtigkeit wegen sei darauf hingewiesen: Auch die Open-Source-Konkurrenz aus dem Linux-Lager präsentierte sich nicht mehr ganz so jung, laut und frisch wie auf der letztjährigen CeBIT oder auch der Systems in München. Man spürte schon deutlich die „Normalisierung“ des Linux-Markts, was ja nicht unbedingt ein schlechtes Zeichen ist. Trotzdem liebe Microsoft. Ein bisschen mehr Spektakel hätten wir schon erwartet. (fbi)

Microsoft-Partnerstand Eine Fundgrube für jeden an Windows 2000 interessierten Besucher war natürlich der Microsoft-Stand und die darin integrierten Partnerpräsentationen. Die Partnerstände waren in Bereiche wie Dokumentenmanagement, E-Commerce, Kommunikation, Systemmanagement u.a. zusammengefasst.

Durch das Zusammenwachsen der IT-Welt mit den Kommunikationstechnologien entstehen viele Lösungen, die Features aus beiden Richtungen integrieren. Die Anwender des „Ixi-Server-Mobile“ von der deutschen Firma Servonic können sich jederzeit und überall von unterwegs z.B. via Handy in ihr Messaging-System einwählen und die Unified-Nachrichten abrufen und verwalten. Durch die SMTP-Unterstützung können sogar unterschiedliche E-Mail-Systeme genutzt werden. Der



von Microsoft in Exchange mitgelieferte Outlook Web Access ermöglicht dem Benutzer den Zugriff via Web auf sämtliche eingegangenen Nachrichten, E-Mails, Fax-, Kurz- und Sprachnachrichten.

Einem weiteren MS-Partnerunternehmen – der BOV – ist es gelungen, den Zugriff verschiedener Kommunikationsmedien auf zentrale Netzwerkdienste zu ermöglichen. Mobile Technologien wie sie in WAP-Devices oder PDAs Verwendung finden, aber auch konventionelle Netzwerk-PCs, werden in eine Basisplattform für ein Unified-Messaging-System integriert.

Auch bei diesen Lösungen stand die Kompatibilität zu Windows 2000 im Vordergrund. Die BOV führt sogar „W2K-ready"-Zertifizierungen für Fremd-Software in ihren Readiness-Labs durch. Dafür ist ein Vorgang in drei Stufen vorgesehen: eine Prüfung unter Windows NT 4.0, nach einer Migration auf Windows 2000 und nach einer Neuinstallation unter Windows 2000. In einigen Windows-2000-unterstützenden Messaging-Systemen wie z.B. Ferrarifax können beispielsweise Windows-Benutzer automatisch als Faxbenutzer übernommen werden.

Die unter dem Systemmanagement-Logo vertretene DVMB hat als eines der ersten Unternehmen in Deutschland alle zehn Spezialisierungen, die Microsoft für entsprechende Qualifikation und Projekterfahrung in seinen Technologien verleiht, inne. Das auf der CeBIT dargestellte Wissensspektrum des IT-Lösungsanbieters reicht von Exchange, Internet/Intranet über SQL, SMS, SNA und Cluster bis hin zu Terminal Server sowie zu den Zusatzspezialisierungen Knowledge Management, Electronic Commerce und Infrastructure.

Die Easy Software zeigte auf ihrem Stand die Integration des XML-Standards in die Dokumentenmanagement-Lösung Easyware. Durch die Einbindung der Extensible Markup Language erhalten die Anwender einen mobilen und plattformunabhängigen Zugriff auf elektronisch archivierte Dokumente und elektronisch abgebildete Arbeitsvorgänge. Außerdem war auch eine mobile Dokumentenmanagement Anwendung zu sehen, die in Zusammenarbeit mit Ericsson entwickelt wurde. Dank eines neuartigen XML/WML-Gateways können Anwender per WAP-fähigem Mobiltelefon in entfernten Easy-Archiven recherchieren und sich die entsprechend aufbereiteten Dokumente ortsunabhängig direkt auf dem Display ihres Handys anzeigen lassen. (kl)

Speichersysteme im Netz E-Commerce-Systeme und viele andere netzwerkbasierende Systeme beanspruchen immer größere Datenmengen, vor deren Flut man sich mit Hilfe moderner Netzwerkspeichersysteme zu retten versucht. Viele kleine und mittlere Unternehmen sehen sich daher gezwungen, auf kurz oder lang in so genannte Network Attached Storage (NAS) zu investieren. In diese Richtung wird man auch von einigen Hardware-Herstellern geleitet, da aus vielen High-end-Servern die Festplattenspeicher ausgelagert werden.

Der Schritt in Richtung Storage Area Network (SAN) hingegen hörte sich wegen der teureren Komponenten und der benötigten Glasfasertechnologie noch bis vor kurzem wie Zukunftsmusik an. Diese Situation hat sich auf der CeBIT schon sichtbar geändert, denn es gab schon etliche Installationen zu sehen. Eine Entscheidungserleichterung für die Planung einer SAN-Speicherlösung kommt auch aus dem Hause IBM, deren Unternehmensbereich Storage Systems einen finanziell praktikableren Migrationsweg bietet. Durch die Installation eines einsatzfähigen SAN-Teilbereichs, der später stufenweise in ein komplettes SAN umgewandelt werden kann, ist es nun auch für kleinere Unternehmen möglich, eine derartige Speicherlösung anzuschaffen.

TIP
Weitere Produkte und Lösungen, die uns aufgefallen sind, finden Sie in der CeBIT-Nachlese ab Seite 59

Eine weitere Speichervariante ist gemeinsam von mehreren Herstellern aus den Bereichen NAS und SAN in Form einer kombinierten Lösung fertiggestellt worden: Legato Systems, Network Appliance, Quantum/ATL, Spectra Logic, Veritas Software und Vixel entwickelten hierzu gemeinsam auf der Basis von Produkten, die auf Interoperabilität geprüft und zertifiziert sind. Keineswegs abwegig könnte man in diesem Fall von NAS und SAN als sich ergänzende Technologien sprechen. Die SAN-basierte Fibre-Channel-Lösung besteht hier aus einem Shared-Tape-Backup-System, das die Netapp Filer von Network Appliance unterstützt und von einer Enterprise-Data-Storage-Software verwaltet wird. Tape Backup ohne LAN und das Sharen von Bändern führen dazu, dass der Backup Traffic aus dem LAN abgezogen wird und eine kostengünstigere Methode denkbar ist.

Auf der CeBIT wurden auch einige neue Bandspeichertechnologien vorgeführt; bei Hewlett-Packard gab es sogar einige Prototypen zu sehen, allerdings nur hinter verschlossenen Türen. Storage-Spezialist Ecrix zeigte auf ihrem Stand ihre innovativen VXA-1-Bandlaufwerke. Die Geräte sind nicht nur auf schnelles Backup ausgelegt, sondern vor allem auf die absolut sichere Wiederherstellung von Daten im Katastrophenfall. Die VXA-1-Laufwerke schreiben und lesen die Daten als individuell adressierte Pakete, auf die sich beim Rücksichern direkt zugreifen lässt. Dadurch wird das Restore beschleunigt und die Fehlerrate verringert. (kl)

Von WAP zum M-Commerce Durch die Annäherung der IT- und Telekommunikationsbereiche verschiebt sich der Trend immer mehr von der reinen Sprachübertragung hin zu Multimedia- und Datendiensten. Die Übertragungsraten für Daten in GSM-Mobilfunknetzen sollen in Zukunft von Technologien wie HSCSD (High Speed Circuit Switched Data) und GPRS (General Packet Radio Services) erheblich gesteigert werden. Auf der CeBIT waren schon die ersten Prototypen der UMTS-(Universal-Mobile-Telephone-System-)Endgeräte zu sehen. Der elektronische Handel soll in Zukunft nicht nur vom fest installierten PC, sondern auch von unterwegs möglich sein. Voraussetzung für den so genannten „M-Commerce" (Mobile Commerce) sind die neuen WAP-(Wireless-Application-Protocol-)Handys, mit denen man mobil auf das rasant wachsende Angebot von WAP-Diensten zugreifen kann. Spätestens auf der CeBIT 2001 werden wir die Erfolge der diesjährigen Ansätze beurteilen können; jetzt schon scheiden sich die Geister nämlich, ob WAP nicht nur eine Eintagsfliege ist und ob Windows 2000 fähig ist, den Durchbruch ins High-end-Computing zu schaffen. (kl)

Win-2000-Launch zwischen Party und Gerichtssaal

Microsoft hat es tatsächlich geschafft und den Termin nicht in letzter Sekunde abgesagt wie manche hartgesottenen Skeptiker vorhergesagt hatten: Seit dem 17. Februar ist Windows 2000 offiziell fertig und seit der CeBIT auch hierzulande zu kaufen.

Der offizielle Launch-Event in San Francisco fiel ganz so aus wie man sich dies angesichts der Bedeutung, die Microsoft dem neuen Betriebssystem für die eigene Zukunft beimisst, vorstellt. 5000 Besucher lauschten dem frisch gebackenen Chief Software Architect Bill Gates, Star-Trek-Captain Patrick Stewart hatte einen Auftritt, und die Rock-Legende Carlos Santana sorgte für den richtigen Sound. Zudem wurde auch gleich noch Windows 2000/64 angekündigt, das Intels kommenden 64-Bit-Prozessor Itanium unterstützen wird sowie ein Embedded Windows 2000 für den Einsatz in Industrierechnern oder Thin Clients.

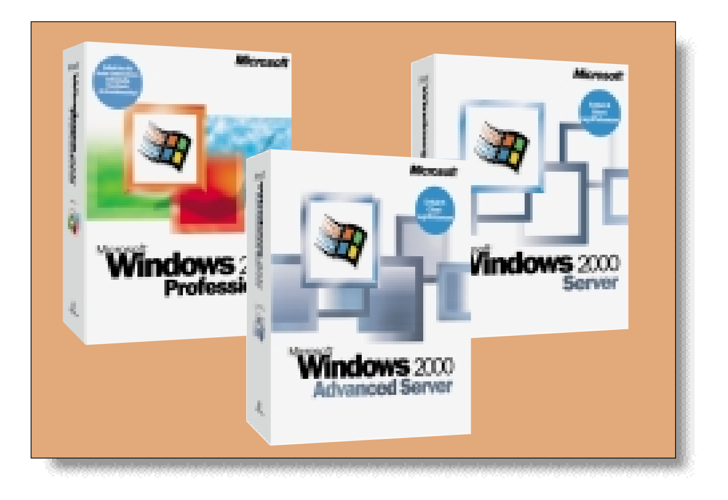
Wer sich eine ähnlich aufwendige Veranstaltung zum Windows-2000-Launch in Deutschland erwartet hatte, wurde allerdings enttäuscht. Zwar veranstaltete Microsoft am Vorabend der CeBIT eine Pressekonferenz, und Windows 2000 war gut auf der Agenda der Firmenvorträge in Hannover vertreten. Doch spektakulär konnte man das wirklich nicht nennen.

Aber selbst in USA wurde von vielen die Markteinführung als recht leise aufgefasst. Vielleicht hat sich Microsoft bewusst zurückgehalten, damit keinesfalls die falschen Leute das neue Betriebssystem kaufen? Auf jeden Fall gab man sich große Mühe, jedem mitzuteilen, dass Windows 2000 auf den Unternehmensanwender zielt und nicht als Windows-98-Nachfolger auf den Consumer-PCs landen soll. Um jeden Missgriff im Ladenregal zu vermeiden, hat Microsoft auf der Packung des deutschen Windows 2000 Professional sogar den Satz „Das zuverlässige Betriebssystem für Unternehmen“ untergebracht.

Wie nicht anders zu erwarten, gab es auch jede Menge kritische Begleitmusik zum Windows-2000-Start. Microsoft gab sich redlich Mühe, die Kritiker mit der notwendigen Munition auszustatten. Genau am Launch-Tag, dem 17. Februar, war schon der erste Fix für das neue Betriebssystem verfügbar. Es galt zwei Sicherheitslücken zu füllen und diverse kleinere Probleme zu beheben. Nichts Dramatisches also, aber Wasser auf die Mühlen derjenigen, die Microsoft keine Qualitätsarbeit zutrauen. Zu allem Überfluss wurde dann noch ein internes Microsoft-Memo bekannt, wonach Windows 2000 angeblich noch 65.000 bekannte Probleme enthalte.

In Deutschland hatte Microsoft mit zwei weiteren Problemen zu kämpfen: Zum einen will die Diskussion um eine mögliche Scientology-Verstrickung von Windows 2000 nicht verstummen. Immer wieder wurde der Verdacht geäußert, mit dem integrierten Programm Diskeeper der Scientology-Firma Executive Software könnten Daten auf den Festplatten von Windows-2000-Rechnern ausgespäht werden. Besonders im öffentlichen Dienst reagierte man auf die Scientology-Connection sehr empfindlich. Microsoft weist darauf hin, dass es in Deutschland kein rechtskräftiges Urteil gebe, das Scientology als verfassungsfeindliche Organisation einstufe. Ausserdem sei der Source-Code von Diskeeper intern geprüft worden, ohne Auffälligkeit festzustellen. Ein Bericht des Nachrichtenmagazins „Der Spiegel“, wonach Microsoft dem Innenministerium angeboten habe, den Windows-2000-Quellcode zu überprüfen, wurde allerdings schnell von Microsoft dementiert.

Weitere Aufregung verursachte eine einstweilige Verfügung des Landgerichts München. Diese richtet sich gegen Einschränkungen der OEM-Version von Windows 2000, die verhindern soll, dass das Betriebssystem auf einem anderen PC installiert wird. Microsoft sieht sich allerdings auf der sicheren Seite. Weder die OEM- noch die Shrinkwrap-Version seien von der einstweiligen Verfügung betroffen. Es werde Microsoft nicht untersagt, geschützte OEM-Versionen zu vertreiben, sondern lediglich solche Windows-Versionen, „...die mit einer Programmsperre ausgestattet sind, die einen Einsatz von Windows nach einem Austausch beliebiger Hardware-Komponenten mit Hilfe einer selbst erstellten Sicherungskopie verhindert.“ Und dies sei bei Windows 2000 nicht der Fall.



Alle skeptischen Stimmen konnten offenbar die Kunden nicht besonders beeindrucken. Bereits Mitte März, einen knappen Monat nach der Markteinführung, meldete Microsoft über eine Million verkaufte Versionen von Windows 2000. Dabei wurden nicht einmal diejenigen Lizenzen gezählt, die über Volumenprogramme an Großkunden gingen. Ganz stolz wies Microsoft bei dieser Gelegenheit darauf hin, dass die Zahl der Support-Anrufe unerwartet gering ausfiele. Man erhalte wesentlich weniger Support-Anrufe pro ausgelieferter Version als bei allen bisher entwickelten Microsoft-Betriebssystemen. (fbi)

Neue Partner erweitern das Leistungsspektrum des WTS-Centers



Eine ganze Reihe neuer Partner konnte das WTS-Testcenter von Group gewinnen. Anwendungen auf Basis von Windows NT Terminal Server sowie Windows 2000 Terminal Services können jetzt auch in einer Umgebung für Application Service Providing (ASP) getestet werden. Mit Unterstützung des neuen WTS-Center-Partners UUnet können Performancetests über das Internet durchgeführt werden, die Rückschlüsse über die Lauffähigkeit der Applikation geben. Im Laufe des Testverfahrens erhalten die Kunden detaillierte Informationen über die erforderliche Leistungsfähigkeit der eingesetzten Server, Router, Switches und aller Netzwerkkomponenten in der geplanten Infrastruktur.

Das Dienstleistungsangebot des WTS-Centers richtet sich sowohl an Unternehmen, die mit Windows Terminal Servern ganze Server-Farmen für interne Netzwerke aufbauen möchten wie auch an Dienstleister (zum Beispiel Internet-Provider oder Rechenzentren), die Applikationen auf Mietbasis über das Internet anbieten möchten.

Die im Testcenter durch den ebenfalls neuen Partner Cisco installierten Switches und Router werden sowohl für Applikationstests als auch Pilotierung von ASP-Umgebungen eingesetzt. Soll die Leistungsfähigkeit einer Server-Farm getestet werden, können die Datenströme in der Testumgebung zwischen den WTS-Servern und Datenbank- oder Fileservern mit den Cisco-Management-Tools genau getestet werden.

Auf besonderes Interesse dürften auch die erweiterten Möglichkeiten stoßen, die durch den neuen Partner T-Mobil eröffnet werden. Durch den Zugriff auf den Windows Terminal Server über die mobilen



T-D1-Datendienste kann auch getestet werden, wie sich die Applikationen beim Zugriff über Wireless Mobile Computing verhalten. (fbi)

WTS-Testcenter
Tel.: 07 21/49 01-116

Kostenlose IBM-Software für Windows-2000-Entwickler

Wer so viele eigene Betriebssysteme besitzt wie IBM, tut sich manchmal schwer, eine eindeutige Strategie zu entwickeln. Außerdem will auch noch die Open-Source-Community mit einem klaren Commitment zur Linux-Unterstützung versorgt werden. Dennoch will Big Blue massiv in das neue Betriebssystem von Microsoft investieren. IBM war nicht nur als einer der „Global Launch Partner“ beim weltweiten Windows-2000-Start prominent vertreten, sondern kündigte zahlreiche Windows-2000-Initiativen an. Natürlich spielt W2K für die Hardware-Division eine wichtige Rolle. Zukünftig werden viele PCs, Laptops und Server mit vorinstalliertem Windows 2000 angeboten. Bestehende NT-4.0-Anwender sollen eine kostenlose CD-ROM mit Treibern, BIOS-Updates und Installationshinweisen zur einfachen Migration auf Windows 2000 erhalten. IBMs Software-Palette, von DB2 über Websphere bis zu MQSeries ist entweder bereits Windows-2000-fähig oder soll dies in Kürze werden.

Ein interessantes Angebot hält IBM für Entwickler bereit, die auf Basis der IBM-Produkte eigene Anwendungen schreiben. Sie können ab 31. März kostenlos eine komplette Suite von Anwendungen von der Website der „IBM Partner World for Developers“ herunterladen (www.developer.ibm.com). Diese enthält unter anderen DB2, Version 6.1, Lotus Domino R5, den Application Server Websphere und die Entwicklungsumgebung Visual Age for Java. (fbi)



IBM
Tel.: 018 03/31 32 33

Banyan setzt ganz auf Windows 2000

Banyan hatte mit Streettalk einen hoch skalierbaren Verzeichnisdienst, als man bei anderen Firmen noch nicht einmal das Konzept verstanden hatte. Doch Streettalk konnte sich – sieht man von einigen Großunternehmen ab – nicht am Markt durchsetzen. Jetzt will sich Banyan mit seinem Verzeichnisdienst-Know-how als Berater im Active-Directory-Markt positionieren. Als nach eigenen Angaben erstes weltweit agierendes Unternehmen migrierte Banyan komplett auf Windows 2000 Server und Active Directory. Mit diesem kundennahen Szenario will Banyan seine Beratungskompetenz demonstrieren und die eigenen Erfahrungen mit der neuen Umgebung vertiefen. (fbi)

Banyan
Tel.: 089/99 02 24-13

EMC verstärkt Zusammenarbeit mit Microsoft

Der Speicherspezialist EMC hat angekündigt, seine strategische Kooperation mit Microsoft zu verstärken und dabei umfassend Windows 2000 zu unterstützen.

Als nach eigenen Angaben erster Anbieter bietet EMCs Data General Division eine garantierte Verfügbarkeit von 99,9 Prozent für Windows 2000 an. Die Garantie gilt für Cluster von DG-Servern, die unter Windows 2000 Advanced Server oder Datacenter Server laufen. Außerdem will EMC gemeinsam mit dem Microsoft Premier Support Services einen globalen Rund-um-die-Uhr-Support für seine Kunden bereitstellen. (fbi)

EMC Computer-Systems Deutschland GmbH
Tel.: 0 61 96/47 28-118

Andersen Consulting und Microsoft gründen Joint Venture

„Avanade“ soll das Unternehmen heißen, mit dem Andersen Consulting und Microsoft gemeinsam den E-Business-Markt bedienen wollen. Das Joint-Venture, in das beide Unternehmen zusammen eine Milliarde Dollar einbringen werden, will neue Internet-basierte Business-Anwendungen auf der Plattform Windows 2000 anbieten. Zielgruppe der Aktivitäten sind sowohl die weltweit 500 größten Unternehmen als auch Internet-Startups und -Spin-offs. Microsoft-Chef Steve Ballmer sieht in der Kombination von Microsofts Technologiestärke mit Andersens Beratungs- und Branchen-Know-how die Hauptvorteile. Dem neuen Unternehmen wird Mitchell Hill, Geschäftsführer von Andersen Consulting, vorstehen. In den kommenden zwei Jahren sollen mehr als 3000 Consultants eingestellt werden. (fbi)

Andersen Consulting
Tel.: 0 61 96/57-66 25

Branchen-Ticker

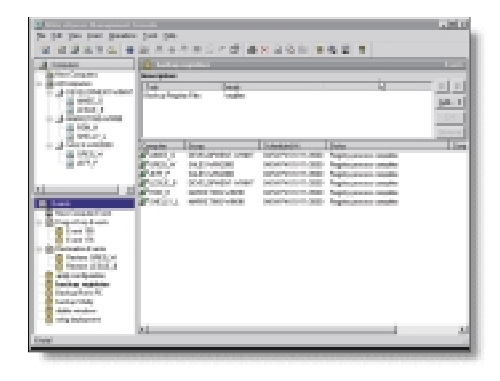
Host-Connectivity-Spezialist **WRQ** hat **Supernova** übernommen, den niederländischen Hersteller einer Enterprise-Entwicklungsumgebung gleichen Namens. WRQ will damit seine strategische Neuausrichtung als Anbieter von E-Business-Lösungen unterstreichen.

Die bislang größte Akquisition in der Software-Branche geht wieder einmal auf das Konto von **Computer Associates**. Vier Milliarden Dollar ist die Übernahme von **Sterling Software** wert, Basis des Geschäfts ist ein Aktientausch. Besonders interessant für CA sind Sterlings Speichermanagementlösungen sowie die Entwicklungs-Suite COOL, die mit der OODB Jasmine ii von CA kombiniert werden soll.

Lutz Becker, über zehn Jahre lang deutscher Geschäftsführer beim Antiviren-Spezialisten **Norman Data Defense**, widmet sich neuen Herausforderungen im E-Commerce-Umfeld. Seine Nachfolge tritt der bisherige Vertriebs- und Marketing-Leiter Volker Krause an.

TIP
Weitere Informationen zu den Firmen, die in den Artikeln erwähnt werden, können Sie über den Web-Kennziffern-dienst des Windows 2000 Magazins anfordern. Zudem finden Sie dort alle Links auf die Webangebote der Firmen.
Die Adresse:
www.win2000mag.de/info

Compaq bundelt Migrations-Tools von Altiris



Eine Technologie- und Distributionsvereinbarung hat der Tool-Hersteller Altiris mit Compaq abgeschlossen. Compaq wird zukünftig eine zeitlich begrenzte Version der Imaging- und Deployment-Software Altiris Express in der Version 4.1 auf seiner Website zum Herunterladen zur Verfügung stellen. Außerdem werden, beginnend mit den neuen Ipaq-Systemen, Express-Agenten auf den Compaq-PCs vorinstalliert.

Zweiter Bestandteil der Vereinbarung: Das Migrations-Tool PC Transplant ist in einer auf Compaq-Rechner zugeschnittenen Version ebenfalls auf der Web-Site von Compaq herunterzuladen. Damit lassen sich die Einstellungen eines PCs auf einen neuen Compaq-PC übertragen. Zusätzlich bieten beide Unternehmen eine Pro-Version an, die PCs unterschiedlicher Hersteller unterstützt und weitere Funktionen zur Migrationsunterstützung enthält. (fbi)

Altiris
Tel.: 0 21 62/2 49 79-0

Hardware-Hersteller setzen auf Windows 2000

Bislang zog NT bei den Vorinstallationen klar den Kürzeren gegenüber Windows 95 und 98. Kann Windows 2000 die Vorherrschaft des Consumer-Windows brechen?

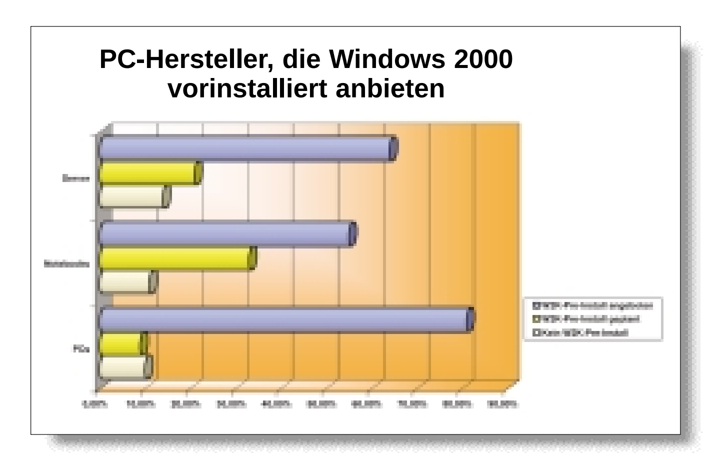


Bild 1. *Über 80 Prozent der befragten Hersteller bieten bereits heute PCs mit vorinstalliertem Windows 2000 an*

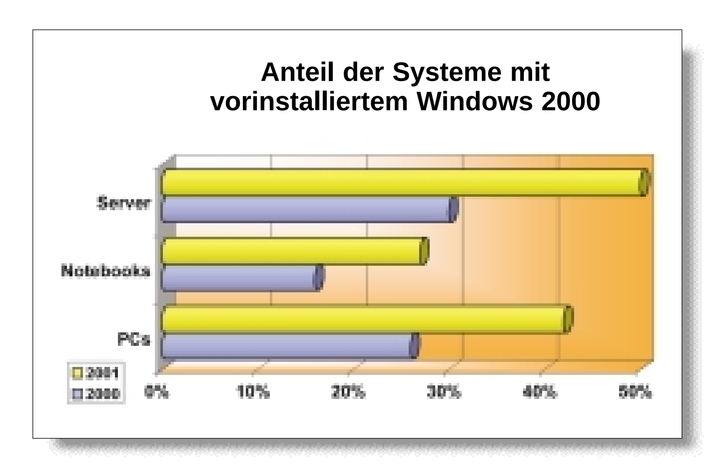


Bild 2. *Für die meisten Hersteller wird Windows 2000 eine wichtige Rolle spielen*

Wie schnell sich Windows 2000 auf dem Markt durchsetzen wird, das hängt nicht zuletzt davon ab, wie oft es zusammen mit neuen PCs, Notebooks und Servern ausgeliefert wird. Bislang konnte sich noch kein Betriebssystem auf dem Markt durchsetzen, wenn es sich nicht auch im OEM-Geschäft etablieren konnte. Das Windows 2000 Magazin führte Anfang März eine Umfrage bei Hardware-Herstellern und -Distributoren im deutschsprachigen Raum durch. Die Ergebnisse lassen einen durchschlagenden Erfolg von Windows 2000 im Markt erwarten.

Schon heute bieten die meisten Hersteller Windows 2000 als vorinstalliertes Betriebssystem für ihre Rechner an. Fast 82 Prozent der Befragten gaben an, dass Windows 2000 als vorinstalliertes Betriebssystem mit ihren PCs zu haben sei. Weitere neun Prozent der Befragten sind noch in der Vorbereitung. Und lediglich knapp zehn Prozent wollen auch in Zukunft ihren Kunden kein Windows 2000 liefern.

Auch bei den Server-Anbietern erreicht Windows 2000 gute Zahlen. Bei immerhin 64 Prozent der Anbieter kann man bereits Windows 2000 vorinstallieren lassen. Weitere 21 Prozent planen ein entsprechendes Angebot. Nur zirka elf Prozent sehen keinen Bedarf für ein vorinstalliertes Windows 2000.

Selbst auf dem Notebook wird Windows 2000 wohl kein Exote sein. Bei 55 Prozent der befragten Anbieter erhält man auf Wunsch bereits ein Windows-2000-Notebook. Mehr als 30 Prozent planen dies für die Zukunft. Auch hier ist mit zirka elf Prozent der Anteil derjenigen Anbieter gering, die auch in Zukunft nicht auf Windows 2000 setzen wollen.

Hohe Erwartungen für die Zukunft

Auf die Frage, wieviel Prozent der ausgelieferten Rechner mit Windows 2000 vorinstalliert werden, haben die meisten Hersteller recht hohe Erwartungen. Noch in diesem Jahr wird Windows 2000 einen festen Platz im Hardware-Geschäft erkämpfen können. Im Durchschnitt rechnen die Anbieter damit, dass 26 Prozent der PCs, 15 Prozent der Notebooks und knapp 30 Prozent der Server mit Windows 2000 ausgestasttet werden. Noch höher die Anteile, die für das nächste Jahr (2001) erwartet werden: 42 Prozent der PCs, 27 Prozent der Notebooks und fast 50 Prozent der Server sollen dann mit dem NT-Nachfolger ab Werk laufen. (fbi)

Einige Kommentare aus der Befragung des Windows 2000 Magazins:

„Da es sich nach den Erfahrungen von Maxdata um das zur Zeit stabilste Betriebssystem handelt, wird der Erfolg nicht lange auf sich warten lassen.“ (Jürgen Werneke, Maxdata)

„Das Top Server System neben Linux und Solaris“ (Gerhard Snoy, Ractech)

„Ohne Freischaltung der Dienste bietet Windows 2000 nur die Funktionen von NT. Es ist vom Preis-Leistungs-Verhältnis zu teuer. Die Probleme mit der Software sind unbekannt.“ (Petra-Isabell Lübcke, Köhler Ingenieurbüro)

„Mit Windows 2000 steht dem Anwender ein Produkt zur Verfügung, welches zum einen einfach zu handeln ist und zum anderen viele interessante und nützliche Features für Unternehmen bietet.“ (Robin Wittland, Wortmann AG)

„Windows 2000 wird den Hardware-Markt massiv verändern. Dank der integrierten Terminal-Services können auch alte PCs und schlanke Endgeräte wie Thin Clients Windows 2000 problemlos nutzen. Der Zwang zu ständiger Aufrüstung entfällt.“ (Andreas Winkler, GTS-GRAL)

SOHO-Internet-Anbindung mit Windows 2000 und NAT

Kostengünstig ins Internet

von Zubair Ahmad

Einen einzelnen Rechner ans Internet anzubinden, ist kein Problem. Schon anspruchsvoller wird es, wenn ein kleines Netzwerk über eine günstige Wählleitung mit dem weltweiten Netz kommunizieren soll. Mit der integrierten Network Address Translation ist in Windows 2000 bereits das richtige Werkzeug an Bord. Besonders, wenn auch noch eine sichere Verbindung zum zentralen Firmennetz aufgebaut werden soll.



In Windows 2000 Server (Win2K Server) bietet Microsoft zwei Methoden zur Herstellung einer Verbindung von SOHO-Netzwerken zum Internet an: Es kann eine Routing-Verbindung oder eine übersetzte Verbindung eingerichtet werden. Bei Routing-Verbindungen fungiert der Win2K-Server als IP-Router und leitet Pakete von SOHO-Clients an die Host im Internet weiter. Über Routing-Verbindungen können Server sämtlichen IP-Verkehr an das Internet weiterleiten. Allerdings sind zur Einrichtung von Routing-Verbindungen Kenntnisse über IP-Netzwerke und Routing notwendig. Bei übersetzten Verbindungen fungiert der Win2K-Server als IP-Router und übersetzt Pakete von SOHO-Hosts an Internet-Hosts. Im Unterschied zu Routing-Verbindungen können Server über die übersetzten Verbindungen möglicherweise nicht sämtlichen IP-Verkehr übersetzen.

In Win2K Server kann Microsofts Internet Connection Sharing (ICS) oder Network Address Translation (NAT) zur Konfiguration übersetzter Verbindungen zum Internet verwendet werden. ICS ist ein Feature des Netzwerk- und DFÜ-Verbindungs-Tools. NAT ist ein Routing-Protokoll, das über das Fenster für Routing und Remote Access konfiguriert wird, das in Bild 1 zu sehen ist. NAT ist die Microsoft-Variante des Network-Address-Translator-Standards der Internet Engineering Task Force (IETF), die eine Internet-Konnektivität auf eine einfache, flexible und kostengünstige Weise bereitstellt. Microsoft bezeichnet mit ICS nun das Merkmal, das zuvor als Shared Access bezeichnet wurde, während NAT in frühen Build-Versionen von Win2K unter dem Namen Connection Sharing bekannt war.

Der Hauptzweck der ICS- und NAT-Dienste besteht darin, eine Netzwerkverbindung für den gemeinsamen Zugriff bereitzustellen, die als Gateway oder Router zur Herstellung einer transparenten Internet-Konnektivität für Clients in einem einzelnen Subnet fungiert. Die Clients im internen Netzwerk benötigen keine Modems, keine zusätzlichen Telefonleitungen oder gültigen IP-Adressen, um eine direkte Verbindung zum Internet zu erhalten. Die Clients können einfach auf den NAT-Server als Proxy-Server für den Zugriff auf das externe Netzwerk zurückgreifen.

Im Request for Comments (RFC) 1631 beschreibt die IETF verschiedene Varianten des Network Address Translators (NAT). Zu diesen Varianten gehören

Network Address Translator in der herkömmlichen Form, eine Zweiwege-Variante des Network Address Translators, eine Zwillingsvariante (Twin Network Address Translator), eine Host-Variante sowie eine Host-NAPT-(Network-Address-Port-Translation-)Variante. Die herkömmliche Variante von Network Address Translator ermöglicht Hosts in einem privaten Netzwerk (z.B. einem LAN) den Zugriff auf Hosts in einem externen öffentlichen Netzwerk (z.B. dem Internet). Sie ermöglicht nur Sitzungen mit abgehendem Verkehr aus privaten Netzwerken zum öffentlichen Netzwerk. Die Zweiwege-Variante von Network Address Translator ermöglicht bidirektionale Sitzungen: für eingehenden und abgehenden Verkehr. Die Zwillingsvariante ermöglicht dem Benutzer, Informationen in den IP-Adressfeldern sowohl für die Quelle als auch für das Ziel zu ändern. Zudem kann die Zwillingsvariante verwendet werden, wenn sich Adresszuweisungen in verschiedenen Domänen überlappen. Die Host-Variante des Network Address Translator und Host-NAPT bieten die Möglichkeit, Sicherheitsmechanismen wie IP Security (IPSec) und DNS Security (DNSsec) in einer Umgebung mit dem Network Address Translator zu nutzen.

Die von Microsoft in Windows 2000 implementierte NAT-Variante steht irgendwo zwischen einem herkömmlichen Network Address Translator und der Zweiwege-Version des Network Address Translators. Microsoft hat der eigenen NAT-Version zahlreiche zusätzliche Features hinzugefügt, um die Verwendung benutzerfreundlicher zu gestalten.

Internet Connection Sharing (ICS) Je nach Situation ist es möglich, dass ein Benutzer ICS dem NAT-Protokoll vorzieht. Dabei kann ICS als „Light-Version“ von NAT betrachtet werden. Zur Konfiguration von ICS muss lediglich ein Kontrollkästchen ausgewählt werden, um einen gemeinsamen Internet-Zugriff zu aktivieren.

Zu beachten ist allerdings, dass ICS und NAT sich gegenseitig ausschließen (d.h. nicht gleichzeitig auf derselben Maschine betrieben werden können). Obwohl diese Dienste einem ähnlichen Zweck dienen, besitzt NAT einige Funktionen, mit denen ICS nicht aufwarten kann. Zum Beispiel können in ICS nicht mehrere öffentliche IP-Adressen konfiguriert werden, und ICS bietet auch keine Unterstützung für WINS-Proxy-Agenten. Die ICS-Clients verwenden ein Mixed-node-NetBIOS zur Namensauflösung in einem SOHO-Netzwerk.

Der Sinn von ICS besteht darin, Clients im internen Netzwerk mit der Möglichkeit eines transparenten Zugriffs auf das Internet auszustatten. Der Benutzer, der ICS einrichtet, braucht dabei kein absoluter Netzwerkexperte zu sein. Zur Einrichtung eines ICS-Servers muss der ICS-Computer mindestens über zwei Schnittstellen verfügen. Eine dieser Schnittstellen muss eine Netzwerkkarte, die andere eine beliebige andere Schnittstelle (wie z.B. Wähladapter, DSL-Adapter, eine andere NIC oder ein ISDN-Adapter) sein. ICS wird an der externen Schnittstelle aktiviert. Bei der ICS-Konfiguration der externen Schnittstelle wird die interne Schnittstelle auf dem ICS-Server automatisch mit der IP-Adresse 192.168.0.1 und der Subnetzmaske 255.255.255.0 konfiguriert.

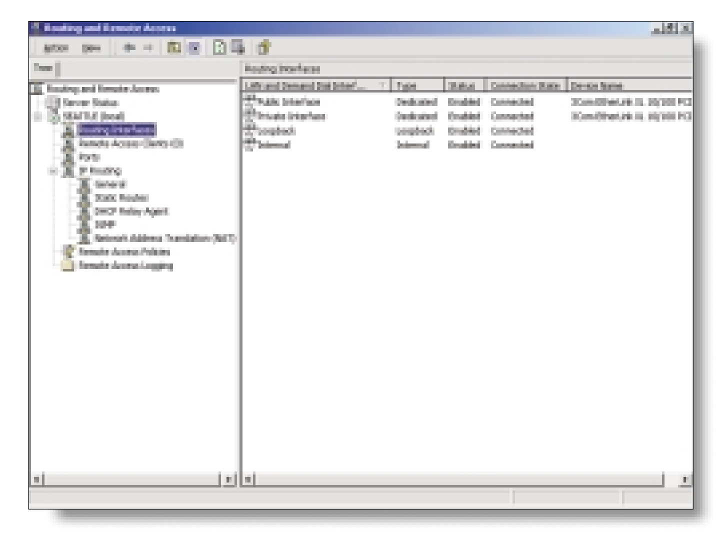


Bild 1. *Das Fenster für Routing und fernen Zugriff*

Außerdem können die Clients so konfiguriert werden, dass sie eine IP-Adresse von einem DHCP-Server empfangen. Der ICS-Server weist den privaten Clients automatisch IP-Adressen aus dem Netzwerkbereich der Klasse C (d.h. 192.168.0.0 bis 192.168.255.255) zu, und die Clients erhalten automatisch die IP-Adresse des ICS-Servers zur DNS-Namenauflösung. Keiner dieser Parameter auf dem ICS-Server ist konfigurierbar. Daher können die DNS-Proxy-Dienste nicht deaktiviert, der Bereich von IP-Adressen, die den Clients zugewiesen werden, nicht geändert, Port-Zuordnungen nicht konfiguriert oder die Zuweisung durch den DHCP-Dienst nicht deaktiviert werden. Tabelle 1 auf Seite 26 enthält eine typische ICS-Client-Konfiguration für ein privates Netzwerk.

Zur Konfiguration von ICS für eine Wählverbindung in Win2K wählt der Benutzer „Start“, „Einstellungen“ und dann „Netzwerk- und DFÜ-Verbindungen“ aus. Anschließend klickt er auf die Option zum Erstellen einer neuen Verbindung. Mit Hilfe des Assistenten für Netzwerkverbindungen wird ein entsprechender Netzwerkverbindungstyp ausgewählt, wie in Bild 2 zu sehen ist. Zum Beispiel kann ein privates Netzwerk angewählt werden (dazu muss eine Nummer in das Dialogfeld für die zu wählende Telefonnummer eingegeben werden). Das Dialogfeld zur Verbindungsverfügbarkeit bietet zwei Optionen für die Verbindung: für alle Benutzer oder nur für den aktuellen Benutzer. Im folgenden Dialogfeld kann das Kontrollkästchen zur Aktivierung von Internet Connection Sharing für diese Verbindung ausgewählt werden, wie in Bild 3 zu sehen ist. Zur Konfiguration von ICS muss der LAN-Adapter im privaten Netzwerk auf 192.168.0.1 gesetzt werden. Eine eingeblendete Warnmeldung informiert über die Konsequenzen, wenn andere Clients im SOHO-Netzwerk einen anderen Adressbereich verwenden. ICS sollte bei der Konfiguration nur für die externe Schnittstelle aktiviert werden. Eine fehlerhafte Konfiguration von ICS kann dazu führen, dass Clients außerhalb des SOHO-Netzwerks (z.B. andere DSL-Benutzer in der Umgebung) IP-Adressen vom DHCP-Dienst erhalten. Wenn ein Computer nicht länger als ICS-Server fungieren soll, kann die Auswahl des Kontrollkästchens zum Aktivieren von Internet Connection Sharing für diese Verbindung im Dialogfeld der Eigenschaften für die Netzwerkschnittstelle zurückgenommen werden.

Firmen, die ein sehr kleines Netzwerk betreiben und sich den Luxus eines Netzwerkadministrators nicht erlauben, können ICS leicht konfigurieren und auf das Internet von den Netzwerk-Clients aus zugreifen, ohne weitreichende Kenntnisse über TCP/IP, DNS, WINS oder eine Browser-Konfiguration zu besitzen. SOHO-Unternehmen könnten eine solche Lösung vorteilhaft einsetzen. Wenn die Umgebung jedoch einer differenzierteren Steuerung unterworfen werden soll, muss NAT anstelle von ICS verwendet werden.

Network Address Translation (NAT) NAT bietet alle Funktionen, die ICS anbietet und darüber hinaus noch weitere. NAT verfolgt die Adress- und Port-Übersetzungen für abgehende Verbindungen, sodass die richtigen Clients im privaten Netzwerk die Pakete aus dem externen Netzwerk zurückerhalten. Zur Bereitstellung der Adressübersetzung für die internen Clients in einem Netzwerk übersetzt NAT die privaten IP-Adressen in den IP-Headern in eine einheitliche öffentliche Adresse. Der Zugriff der Clients auf das Internet erfolgt transparent und ohne zusätzliche Software. Der NAT-Server fungiert als Router und kann zudem TCP- oder UDP-Ports für die Clients übersetzen. Diese Funktionsbeschreibung klingt vielleicht den Diensten ähnlich, die von Microsoft Proxy Server angeboten werden. Obwohl die beiden Dienste Unterschiede aufweisen, stellen sie doch eine ähnliche Funktionalität bereit. Ein NAT-Server ist jedoch keine Alternative zum Proxy Server.

Zur Installation von NAT unter Win2K muss die Option „Verwaltung“ unter „Programme“ im Menü „Start“ ausgewählt werden. Dort muss das Fenster für Routing und RAS geöffnet, der Server hinzugefügt, mit der rechten Maustaste auf den Server-Namen geklickt und dann die Option zum Konfigurieren und Aktivieren von Routing und RAS ausgewählt werden. Nach der Installation von RRAS fordert das Programm den Benutzer auf, den Dienst zu starten. Nach dem Starten des Dienstes muss IP-Routing geöffnet und mit der rechten Maustaste auf „Allgemein“ geklickt werden. Hier muss die Option für ein neues Routing-Protokoll und dann Netzwerkadressübersetzung (NAT) ausgewählt und anschließend auf OK geklickt werden (Bild 4). Im nächsten Schritt müssen unter „IP-Routing“ die Option Netzwerkadressübersetzung (NAT) mit der rechten Maustaste angeklickt und anschließend die Schnittstellen (mindestens zwei) hinzugefügt werden.

Bild 5 zeigt eine typische SOHO-Konfiguration mit zwei Netzwerkkarten (NICs). „Private NIC“ stellt die interne Schnittstelle dar und arbeitet mit der statischen IP-Adresse 192.168.0.1, um die Verbindung zum Netzwerk herzustellen. „Public NIC“ stellt die externe Schnittstelle dar, die mit einer DSL-Verbindung zu einem Internet-Dienstanbieter (ISP) unter Verwendung einer statischen IP-Adresse für das Internet arbeitet wie zum Beispiel 10.10.10.1. Im Allgemeinen wird diese statische IP-Adresse vom ISP zugewiesen.

Zur Konfiguration einer externen Schnittstelle über das Dialogfeld für Eigenschaften der Schnittstelle wählt man die Registerkarte „Allgemein“, die Option für öffentliche Schnittstelle, die mit dem Internet verbunden ist, aus und klickt auf OK. Zur Konfiguration einer internen Schnittstelle ist wiederum die Registerkarte „Allgemein“ und dann die Option für private Schnittstelle, die mit dem privaten Netzwerk verbunden ist, auszuwählen. Diese beiden Optionen schließen sich jeweils gegenseitig aus.

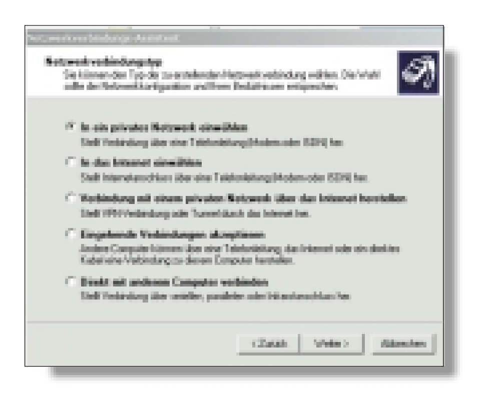


Bild 2. *Auswählen eines Netzwerkverbindungstyps*

Nun können zusätzliche Optionen für NAT konfiguriert werden. Nach dem Klicken auf Netzwerkadressübersetzung (NAT) mit der rechten Maustaste und der Auswahl von „Eigenschaften“ stehen vier Registerkarten zur Konfiguration

zur Verfügung: Allgemein, Übersetzung, Adresszuweisung und Namenauflösung. Die Registerkarte „Allgemein“ enthält vier Protokollieroptionen, die weitgehend selbsterklärend sind. Mit diesen Optionen können Ebenen der Protokollierung für die Ereignisanzeige von Win2K definiert werden.

Die Registerkarte „Übersetzung“ ermöglicht die Festlegung von Zeitlimitwerten für TCP- und UDP-Sitzungen und die Angabe, wie lange eine dynamische Zuordnung für eine TCP- oder UDP-Sitzung in der internen Routing-Tabelle des NAT-Servers verbleibt. Der Standardwert für verbindungsorientierte TCP-Sitzungen beträgt 1440 Minuten (24 Stunden), der Standardwert für verbindungslose UDP-Sitzungen ist eine Minute.

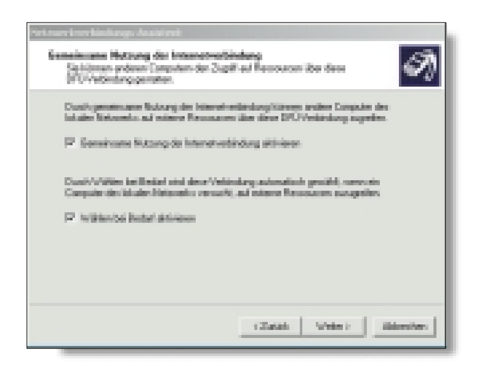


Bild 3. *Aktivieren von ICS*

Die Registerkarte für Adresszuweisung, die in Bild 6 zu sehen ist, ermöglicht eine automatische Zuordnung von IP-Adressen für die internen Clients. Durch die Auswahl des Kontrollkästchens zur automatischen Zuordnung von IP-Adressen über DHCP wird die DHCP-Zuweisungsfunktion aktiviert. Zur Vermeidung doppelter IP-Adressen im internen Netzwerk kann mit Hilfe der Option Ausschließen ein Bereich von IP-Adressen, die im privaten Netzwerk bereits benutzt werden, ausgeschlossen werden. Microsoft empfiehlt, die IP-Adresse des NAT-Servers der Liste der reservierten IP-Adressen hinzuzufügen. Die Registerkarte für Adresszuweisung erweckt den Anschein, als ob ein DHCP-Server im privaten Netzwerk erforderlich wäre, weil aus dem Dialogfeld hervorgeht, dass diese Option konfiguriert wird, um DHCP zur automatischen Adresszuweisung zu verwenden. Tatsächlich ist jedoch kein DHCP-Server im privaten Netzwerk erforderlich. Wenn das Kontrollkästchen zur automatischen Zuordnung von IP-Adressen über DHCP ausgewählt wird, wird eine DHCP-Zuweisungsfunktion aktiviert, die praktisch als eingeschränkter DHCP-Server fungiert.

Die Registerkarte für Namenauflösung ermöglicht eine Auflösung von Namen in Adressen entweder für Windows- oder für TCP/IP-Netzwerk-Clients. Der NAT-Server kann als ein DNS- oder WINS-Proxy-Agent für die privaten Clients fungieren. Der WINS-Proxy-Dienst, der von dem NAT-Server bereitgestellt wird, ist nicht mit dem WINS-Proxy-Dienst identisch, der in Windows-NT-Versionen verfügbar ist. NAT konfiguriert die Clients automatisch mit der IP-Adresse des NAT-Servers als deren WINS-Server. In einem SOHO-Netzwerk lautet die WINS-Server-Adresse 192.168.0.1 (siehe Tabelle 1). Der zweite Unterschied besteht darin, dass die Clients nur annehmen, dass der Server ihr WINS-Server ist. Der NAT-Server fragt den WINS-Server-Satz in seiner IP-Konfiguration ab und gibt die Ergebnisse an die Clients zurück. (Der Client fragt den WINS-Server ab, er registriert seine Adresse aber nicht beim WINS-Server.)

Der WINS-Proxy-Dienst in NAT löscht Client-Namensregistrierungen, sodass die Datensätze nicht in der WINS-Datenbank verbleiben. Da die Clients sich nie beim WINS-Server im privaten Netzwerk registrieren, kann die Verbindung zu einem privaten Client über den Namen (z.B. \\server\freigabename) möglicherweise nicht hergestellt werden. Aus diesem Grund muss es im privaten Netzwerk eine Methode zur Auflösung von Namen geben. Eine Lösung besteht in der Verwendung von IP-Adressen anstelle von Namen, um die Verbindung zu anderen Maschinen (z.B. \\192.168.0.3\data) herzustellen. Eine andere Möglichkeit wäre die Verwendung der Datei LMHOSTS. Zur Zuweisung einer WINS-Adresse an einen Client ist aber DHCP empfehlenswert.

Der DNS-Proxy funktioniert ähnlich wie ein WINS-Proxy, wobei die Clients DNS-Abfragen an den NAT-Server senden. Um auf die Client-Abfragen reagieren zu können, fragt der NAT-Server seinerseits den DNS-Server-Satz in seiner IP-Konfiguration (z.B. den DNS-Server eines Internet-Dienstanbieters) ab und liefert die Ergebnisse an die Clients zurück. Sofern diese Option nicht aktiviert ist, haben die Clients im privaten Netzwerk keine Möglichkeit, Host-Namen im Internet aufzulösen (wenn nicht eine alternative Methode zur Bereitstellung von Namenauflösung eingerichtet wurde). Wenn dies erwünscht ist, kann der NAT-Server zu einem DNS-Server gemacht werden. Für den Fall, dass der Server die DNS-Abfragen nicht auflösen kann, ist es sinnvoll, den DNS-Server zur Weiterleitung von Anforderungen an einen anderen DNS-Server, zum Beispiel an den DNS-Server eines Internet-Dienstanbieters, zu konfigurieren.

DHCP-Zuweisungsfunktion NAT und ICS enthalten eine DHCP-Zuweisungsfunktion, die wie ein DHCP-Server arbeitet. Die DHCP-Zuweisungsfunktion vergibt Leases von IP-Adressen an die Clients aus einem Adressbereich, der über die Registerkarte zur Adresszuweisung konfiguriert wird. Die DHCP-Zuweisungsfunktion lässt sich als eine eingeschränkte Form von DHCP (DHCP „light“) auffassen. Im Unterschied zum DHCP-Server besitzt die DHCP-Zuweisungsfunktion keine konfigurierbare Datenbank. Alle Parameterkonfigurationen für die DHCP-Zuweisungsfunktion einschließlich der DNS- und WINS-Proxy-Parameter erfolgen automatisch. Obgleich jeder beliebige Bereich von IP-Adressen an der internen Schnittstelle mit der DHCP-Zuweisungsfunktion verwendet werden kann, empfiehlt es sich, nur Routing-fähige private IP-Adressbereiche zu verwenden wie sie in RFC 1918 definiert werden.

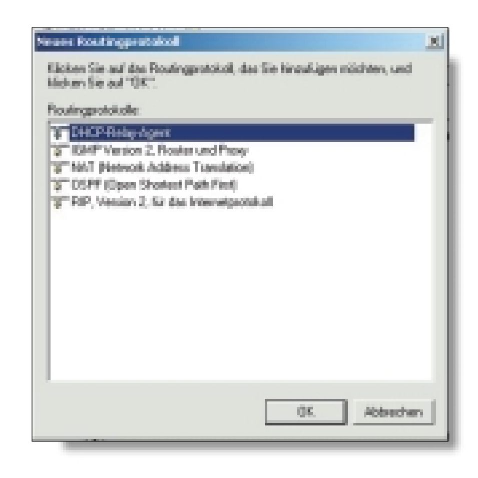


Bild 4. *Hinzufügen des NAT-Routing-Protokolls*

Der Standardbereich für Netzwerk-IDs in NAT ist ein Bereich, an dem Microsoft Änderungen in Win2K Beta-Versionen vorgenommen hat. Eine frühe Build-Version arbeitete mit einem Adressbereich der Klasse C. In späteren

Build-Versionen beschloss Microsoft, einen Bereich für private Netzwerk-IDs der Klasse B (169.254.0.0 bis 169.254.255.255) zu verwenden. Microsoft wechselte zu diesem Bereich der Klasse B, weil die Win2K- und Windows 98-Clients diesen Bereich zur automatischen IP-Konfiguration verwenden und sich die Kommunikation einfacher gestaltet, wenn NAT mit diesem Bereich arbeitet. In Win2K RC2 kehrte Microsoft zur Klasse C als Standardbereich für IP-Adressen zurück wie in Bild 6 zu erkennen ist. Die DHCP-Zuweisungsfunktion gibt mehrere IP-Konfigurationsoptionen an Clients aus. Tabelle 1 zeigt eine Standardkonfiguration für einen NAT-Client in einem privaten Netzwerk.

Die Informationen zur DHCP-Zuweisungsfunktion und zum DNS-Proxy können durch Klicken mit der rechten Maustaste auf Netzwerkadressübersetzung (NAT) im Fenster für Routing und RAS angezeigt werden. Außerdem kann zur Verwaltung von IP-Einstellungen der Befehl Netsh verwendet werden. Wenn Netsh ausgeführt wird, kann zum Beispiel Folgendes eingegeben werden:

```
routing ip autodhcp show global
```

Durch diesen Befehl werden die Konfigurationsinformationen der DHCP-Zuweisungsfunktion (DHCP Allocator) angezeigt. Die verfügbaren Befehlsoptionen können durch Ausführen von Netsh und der Eingabe eines Fragezeichens (?) angezeigt werden.

Wie verhält es sich nun, wenn ein DHCP-Server im internen Netzwerk eingesetzt werden soll? Führt die Verwendung von DHCP zu Konflikten? Wenn im Netzwerk Router, DNS-Server oder DHCP-Server vorhanden sind, kann es zu einigen Problemen kommen. Der NAT-Server versucht in diesem Fall, diese konkurrierenden Dienste zu erkennen, und falls ihm dies gelingt, beendet er die eigenen Dienste. Der NAT-Server arbeitet mit Paketen der Formate Internet Control Messaging Protocol (ICMP) Router Solicitation und DHCP Discover, um diese Dienste zu erkennen.

Um den DHCP-Server auf dem Win2K-Server anstelle der DHCP-Zuweisungsfunktion zu verwenden, muss das Kontrollkästchen für die automatische Zuordnung von IP-Adressen mit DHCP ausgewählt werden, das in Bild 6 zu sehen ist. Für die Nutzung des DHCP-Servers sprechen verschiedene Gründe. Ein DHCP-Server unter Win2K kann Clients einer früheren Version bei dem DDNS-Server (Dynamic DNS) von Win2K dynamisch registrieren. Ein DHCP-Server bietet zudem eine Steuerung von DHCP-Optionen, die von der DHCP-Zuweisungsfunktion nicht angeboten werden wie zum Beispiel die Bereitstellung eines Domänennamens für die Clients oder die Änderung der IP-Lease-Dauer. Sie können außerdem einen anderen DHCP- oder WINS-Server zuordnen. Die Verwendung von DHCP zur Zuordnung eines WINS-Servers zu Clients ermöglicht eine einfachere Namenauflösung für interne Clients. Wenn statt dessen der WINS-Proxy-Dienst verwendet wird (anstatt die Adresse eines WINS-Servers über DHCP-Optionen an Clients weiterzugeben), werden die Clients nicht registriert, und der Dienst kann Namen nicht auflösen. Wenn die Adresse eines WINS-Servers als Teil der DHCP-Optionen definiert wird, werden die Clients beim WINS-Server registriert, und die Namenauflösung wird transparent.

Beim Einsatz eines DNS-Servers verwendet der Autor DHCP-Optionen, um die IP-Adresse des DNS-Servers seines Internet-Dienstanbieters an die privaten Clients zu liefern, die mit DHCP-Optionen arbeiten. Wenn ein DHCP-Server anstatt der DHCP-Zuweisungsfunktion verwendet werden soll, kann dazu die Registerkarte für Adresszuweisung unter den NAT-Eigenschaften ausgewählt, die Auswahl des Kontrollkästchens für die automatische Zuordnung von IP-Adressen über DHCP zurückgenommen und ein DHCP-Server im internen Netzwerk installiert werden. Für eine SOHO-Umgebung kann der NAT-Server auch als DNS-, WINS- und DHCP-Server dienen. Die Clients können so konfiguriert werden, dass sie IP-Informationen von einem DHCP-Server empfangen. Tabelle 1 zeigt eine Client-Standardkonfiguration mit einem DHCP-Server.

Paketübersetzung Der NAT-Server muss alle Pakete von einem nicht Routing-fähigen IP-Adressbereich im privaten Netzwerk in eine gültige IP-Adresse im Internet übersetzen. Der Server kann alle IP-Adressen, TCP-Port- und UDP-Portinformationen in den IP-, TCP- bzw. UDP-Headern transparent übersetzen. Wenn jedoch die Anwendung die IP-Adresse, die TCP-Port- oder UDP-Portinformationen in den Header der Anwendung (anstatt in den IP-Header) schreibt, ist der NAT-Server möglicherweise nicht in der Lage, diese Pakete (z.B. FTP-Pakete) richtig zu übersetzen.

Client-IP-Konfigurationen

Adresstyp	ICS-Client-Konfiguration in einem privaten Netzwerk	NAT-Client-Konfiguration in einem privaten Netzwerk	Beispiel für Standardkonfiguration für einen SOHO-Client, der einen DHCP-Server verwendet
IP-Adresse	192.168.x.x	192.168.x.x	192.168.x.x
Subnetzmaske	255.255.255.0	255.255.255.0	255.255.255.0
Standard-Gateway	192.168.0.1 (ICS-Server-Adresse)	192.168.0.1 (NAT-Server-Adresse)	192.168.0.1 (Adresse der internen Schnittstelle des NAT-Servers)
DHCP-Server	NV	NV	192.168.0.1 (NAT-Server-Adresse)
DNS-Server	192.168.0.1 (ICS-Server-Adresse)	192.168.0.1 (NAT-Server-Adresse)	x.x.x.x (DNS-Server-Adresse des ISP)
WINS-Server	NV	192.168.0.1 (NAT-Server-Adresse)	192.168.0.1 (WINS-Server-Adresse)

Eine NAT-Editorkomponente kann Pakete richtig behandeln, die der NAT-Server ansonsten nicht übersetzen kann. Damit die Übersetzung möglich ist, müssen Pakete für NAT-Server eine IP-Adresse im IP-Header, TCP-Port-Nummern im TCP-Header und UDP-Port-Nummern im UDP-Header besitzen. Alle anderen Pakete machen einen NAT-Editor erforderlich. HTTP erfordert keinen NAT-Editor, da für HTTP die Übersetzung einer IP-Adresse in den IP-Header und eines TCP-Ports in den TCP-Header erforderlich ist. PPTP verwendet keine TCP- oder UDP-Header. Stattdessen arbeitet PPTP mit einem GRE-(Generic-Routing-Encapsulation-)Header. Die Tunnel-ID im GRE-Header identifiziert die Daten. Falls NAT die Tunnel-ID innerhalb des GRE-Headers nicht übersetzen kann, kommt es zu Konnektivitätsproblemen. Da NAT Tunnel-IDs für PPTP-Pakete nicht übersetzen kann, wird für eine geeignete Übersetzung ein NAT-Editor benötigt.

Win2K wird mit integrierten NAT-Editoren für FTP, ICMP und PPTP geliefert. Microsoft plant, APIs für NAT-Editoren zur Verfügung zu stellen, damit Dritthersteller weitere NAT-Editoren entwickeln können. Zur Zeit sind aber noch keine NAT-Editoren für IPSec, Lightweight Directory Access Protocol (LDAP), COM, ferne Prozeduraufrufe (RPC) oder SNMP verfügbar.

Zum Einsatz verschlüsselter Anwendungen bzw. von Anwendungen, bei denen sich die IP-Adressen nicht im IP-Header befinden, kann PPTP zum Tunneln durch den Server verwendet werden. Layer 2 Tunneling Protocol (L2TP), das zum Lieferumfang von Win2K gehört, erfordert keinen NAT-Editor, sodass L2TP transparent eingesetzt werden kann. Jedoch kann das Protokoll L2TP nicht mit IPSec verwendet werden, da der Server die Pakete nicht übersetzen kann (für IPSec ist kein NAT-Editor verfügbar). Wenngleich IPSec für die Sicherheit mit NAT nicht verwendet werden kann, ist es möglich, Web-basierte Anwendungen mit Secure Socket Layer (SSL) zu verschlüsseln. Eine Authentifizierung bei einem Win2K-Domänen-Controller über einen NAT-Server ist nicht möglich, da der NAT-Server keine Kerberos-5-Pakete übersetzt, die von Win2K-Domänen-Controllern verwendet werden.

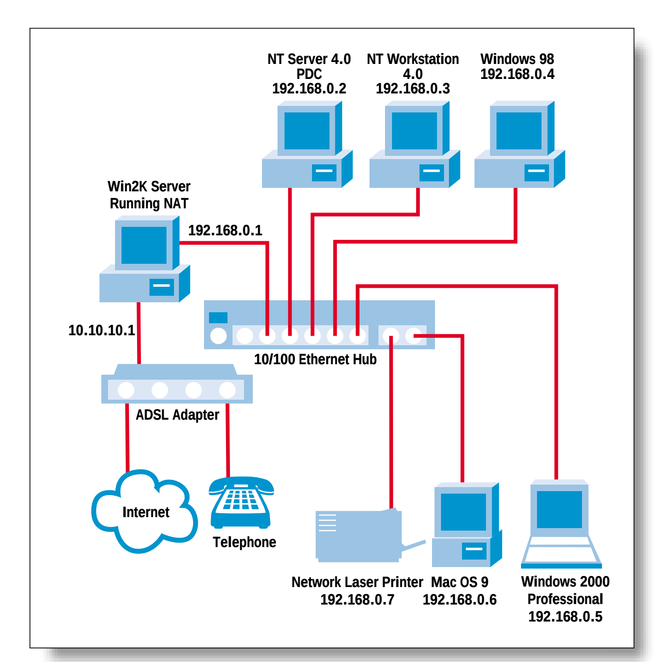


Bild 5. *Konfiguration eines SOHO-Netzwerks*

Adress- und Port-Übersetzung

NAT ermöglicht eine Übersetzung bestimmter Adressen und Ports. In der Regel führt der NAT-Server Adress- und Port-Übersetzungen durch. Darüber hinaus kann der Server für Address Mapping anstatt zu einer Übersetzung konfiguriert werden. Bei der Adresszuweisung können die privaten internen Adressen einem Pool öffentlicher Internet-Adressen zugeordnet werden. Diese Methode ist skalierbarer als die Methode der Adress- und Port-Übersetzung. Die Adresszuweisung ermöglicht eine Zuordnung mehrerer eingehender Verbindungen an den gleichen Port oder Dienst. Allerdings ist die Adresszuweisung recht kompliziert und verlangt vom Internet-Dienstanbieter (ISP) das Hinzufügen statischer Routes für den Pool von IP-Adressen, der vom NAT-Server verwendet wird.

Mit Hilfe der Registerkarte für den Adressenpool des Dialogfelds für die Eigenschaften einer Schnittstelle kann der Server zur Verwendung des Adressübersetzungsmodus konfiguriert werden. Ein Adressbereich kann zur Konfiguration eines Pools von Adressen definiert werden. Clients verwenden dann eine eindeutige öffentliche Adresse aus diesem Pool dynamisch, sofern nicht bestimmte Adressen für spezielle Maschinen reserviert werden. Das Reservieren einer Adresse ist eine Möglichkeit, Verbindungen vom Internet zum privaten Netzwerk bereitzustellen. Daneben kann auch mit einer Spezial-Port-Zuordnung gearbeitet werden. Die Einrichtung der Port-Zuordnung erfolgt über die Registerkarte für Spezial-Ports im Dialogfeld für die Eigenschaften der Schnittstelle.

Vergleich von NAT mit ICS und Proxy Server ICS ist einfach zu konfigurieren und erfordert lediglich die Aus-

wahl eines Kontrollkästchens. Für die manuelle Konfiguration von NAT sind dagegen weitergehende Kenntnisse erforderlich. In einem SOHO-Netzwerk kann ICS mit einem LAN-Adapter verwendet werden. Die zweite Schnittstelle kann ein Modem sein. Ein NAT-Server wird in der Regel mit mehreren Schnittstellen verwendet. Bei ICS kann nur eine öffentliche IP-Adresse genutzt werden. NAT hingegen unterstützt mehrere öffentliche IP-Adressen. ICS unterstützt nur einen festen Bereich von IP-Adressen für Clients im privaten Netzwerk. NAT ermöglicht einen Bereich, der zur Anpassung an die Erfordernisse konfiguriert werden kann. Und schließlich bietet NAT eine Unterstützung sowohl für DNS- als auch für WINS-Proxy-

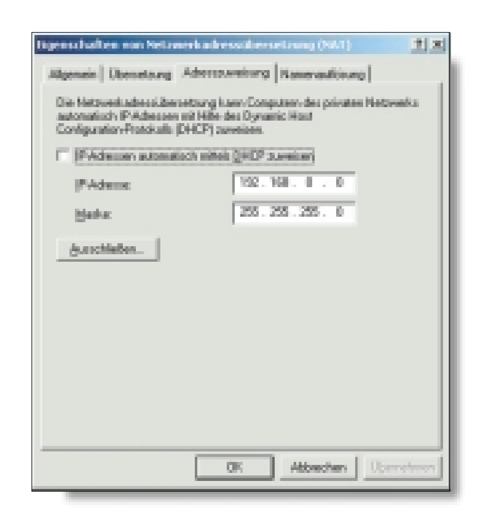


Bild 6. *Konfigurieren der Adresse eines Clients*

Dienste. ICS unterstützt demgegenüber nur DNS-Proxy-Dienste.

NAT und Proxy Server stellen eine in gewisser Hinsicht ähnliche Funktionalität bereit. Beide Dienste ermöglichen einem kleinen privaten Netzwerk oder SOHO-Netzwerk die Verwendung einer Maschine als Proxy, um transparent eine Verbindung zum Internet herzustellen. Für NAT muss keine weitere Software installiert oder konfiguriert werden. Die einzige Voraussetzung besteht darin, dass die Clients für DHCP sensibilisiert wurden (d.h., dass sie zum Empfang einer IP-Adresse von einem DHCP-Server konfiguriert wurden). Für Proxy-Server müssen die Browser der Clients zur Verwendung des Proxy-Servers konfiguriert werden. Die einzige Ausnahme bilden Win2K-Clients, die automatisch nach einem Proxy-Server suchen und den Browser des Clients selbsttätig konfigurieren können.

Ein Proxy-Server kann für SOHO-Netzwerke kostenaufwendiger sein, sodass das Für und Wider abzuwägen ist. In großen oder sicheren Umgebungen ist Proxy-Server aufgrund der überlegenen Filter- und Cache-Funktionen wahrscheinlich die bessere Wahl. Für Heimbüros oder kleinere Netzwerke, in denen die Sicherheitsanforderungen nicht so streng sind, erscheint NAT wegen der einfachen Handhabung, des günstigen Preises und der bequemen Verwaltungsmöglichkeiten vorteilhafter.

NAT ist aus verschiedenen Gründen vorzuziehen. Der Hauptgrund ist der, dass NAT die Verwendung von PPTP von einem NAT-Client aus zur Verbindung mit einem Firmennetzwerk im Internet ermöglicht, wodurch ein sicherer Zugriff auf das Firmennetzwerk zur Übertragung von Dateien, zur Nutzung eines Microsoft Outlook-Clients, zum Drucken oder zur Ausführung angepasster Anwendungen bereitgestellt wird. Ein Proxy-Server gibt einem Proxy-Client keine Möglichkeit, über PPTP einen Tunnel durch einen Proxy-Server herzustellen. Ein Proxy-Server kann lediglich zur Herstellung einer PPTP-Verbindung zu einem Firmennetzwerk verwendet werdet. Ähnlich wie Proxy-Server gibt der NAT-Server dem Benutzer die Möglichkeit, von einem beliebigen Client in einem SOHO-Netzwerk aus SSL für verschiedene Operationen wie zum Beispiel Aktienhandel, Online-Banking oder die Ausführung Web-basierter Anwendungen für E-Commerce), transparent auszuführen.

Gute Gründe NAT wird wahrscheinlich zu einer der bevorzugten Funktionskomponenten für viele Win2K-Benutzer avancieren. Die effiziente, einfache, zuverlässige und kostengünstige Lösung eignet sich gut zur Internet-Konnektivität für Zweigstellen und kleine Netzwerke. NAT besitzt verschiedene Vorteile; Die mögliche Verwendung von PPTP ist ein großer Pluspunkt. Die Filterfunktionen, die Port-Übersetzung und die Wählfunktion auf Anforderung verstärken den positiven Eindruck. Die Möglichkeit, dass in Zukunft zusätzliche NAT-Editoren hinzugefügt werden, macht diesen Dienst sogar noch attraktiver. Benutzer, die Proxy-Server und Lösungen von Drittherstellern prüfen, sollten den NAT-Server von Win2K nicht außer Acht lassen. Vielleicht bietet NAT ja bereits all das, was notwendig ist. (kl)

Das Windows Management Interface

Modernes Systems-Management

von Mark Russinovich

Mit dem Windows Management Interface (WMI) geht Microsoft einen großen Schritt hin zu einer flexiblen und erweiterbaren Middleware für das Systems-Management verteilter Systeme. Mark Russinovich erklärt die neue Architektur und schildert die Vorteile für Entwickler und Administratoren.

Die in NT integrierten Features zur Ereignis- und Leistungsüberwachung erfüllen zwar die ihnen zugedachten Ziele, aber sie besitzen auch Einschränkungen. Zum Beispiel unterscheiden sich die Programmierschnittstellen voneinander, was die Komplexität von Anwendungen erhöht, die sowohl mit Ereignisüberwachung als auch mit Leistungsmessung zur Erhebung von Daten arbeiten. Die Leistung des Performance-API kann gering ausfallen, insbesondere bei Einsatz über das Netzwerk, da dieses API einen Alles-oder-Nichts-Ansatz implementiert. Für eine Anwendung gibt es keine Möglichkeit, die Leistungsinformationen nur spezieller Komponenten abzufragen. Der größte Nachteil der vorhandenen Überwachungseinrichtungen besteht darin, dass sie wenig oder nicht erweiterbar sind und auch keine bidirektionale Interaktion ermöglichen, die jedoch für ein Management-API unabdingbar ist.

Mit dem Windows Management Interface (WMI) vollzieht Microsoft den nächsten Schritt in der von Windows angebotenen Unterstützung für Unternehmensmanagement. WMI ist Microsofts Implementierung der WBEM-(Web-Based-Enterprise-Management-)Technologie. WBEM bezeichnet einen von dem Industriekonsortium Distributed Management Task Force (DMTF) definierten Standard. Der WBEM-Standard umfasst den Aufbau einer erweiterbaren Einrichtung zur Unternehmensdatenerfassung und zum Unternehmensmanagement, die über die Flexibilität und Erweiterbarkeit verfügt, die zur Verwaltung ferner aus willkürlich zusammengestellten Komponenten bestehender Systeme erforderlich sind. Microsoft hat WMI unter Windows 98 implementiert, WMI für NT 4.0 mit Service Pack 4 (SP4) oder einer höheren Version sowie Win95 OSR2 verfügbar gemacht und hat WMI in Windows 2000 (Win2K) integriert. Die WMI-Entwicklung von Microsoft zielt jedoch ganz auf Win2K ab. Mit der Implementierung auf WMI basierender Managementprogramme durch Dritthersteller können Administratoren alle Betriebsfunktionen ihrer Win2K-, NT- oder Win9x-Systeme von einer beliebigen Stelle im Netzwerk aus überwachen und steuern. Dieser Artikel bietet eine Führung in das Innere von WMI. Die meisten der hier beschriebenen Aspekte treffen auf alle Windows-Plattformen zu, die WMI unterstützen. Die Detailbehandlung der Implementierung konzentriert sich jedoch auf Windows 2000.

Die WMI-Architektur Die WMI-Architektur besteht aus vier Segmenten, wie in Bild 1 zu sehen ist: Managementanwendungen, WMI-Infrastruktur, Provider und verwaltete Objekte. Managementanwendungen sind Windows-Anwendungen, die auf Daten, die von den Anwendungen über verwaltete Objekte ermittelt werden, zugreifen und sie darstellen bzw. verarbeiten. Ein einfaches Beispiel einer Managementanwendung wäre eine Ersatzanwendung für den Systemmonitor, die auf WMI und nicht

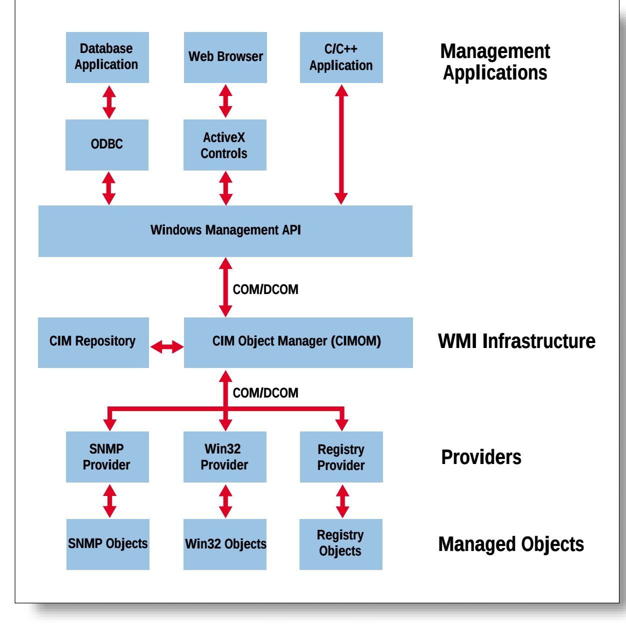


Bild 1. *Die WMI-Architektur*

Provider-Klassifizierungen

Klassifizierung	Beschreibung
Klasse (Class)	Dient zum Abrufen, Ändern, Löschen und/oder Aufzählen einer Providerspezifischen Klasse. Kann außerdem Abfrageverarbeitung unterstützen.
Instanz (Instance)	Dient zum Abrufen, Ändern, Löschen und/oder Aufzählen von Instanzen system- und/oder Provider-spezifischer Klassen. Kann außerdem eine Abfrageverarbeitung unterstützen
Eigenschaft (Property)	Dient zum Abrufen und/oder Ändern einzelner Eigenschaftswerte.
Methode (Method)	Dient zum Aufrufen von Methoden für eine Provider-spezifische Klasse.
Ereignis (Event)	Dient zum Generieren von Ereignisbenachrichtigungen
Ereignisverbraucher (Event Consumer)	Dient der Zuordnung eines physischen Verbrauchers zu einem logischen Verbraucher zur Unterstützung der Ereignisbenachrichtigung

mehr auf das Performance-API zurückgreift, um Leistungsinformationen zu erhalten. Ein komplexeres Beispiel könnte ein Dienstprogramm zum Unternehmensmanagement sein, das Administratoren die Möglichkeit gibt, automatisierte Erstellungen von Inventaren der Soft- und Hardware-Konfiguration jedes Computers im Unternehmen durchzuführen.

Entwickler müssen Managementanwendungen gewöhnlich auf die Erhebung von Daten aus bestimmten Objekten und die Verwaltung dieser Objekte ausrichten. Ein Objekt kann dabei eine Einzelkomponente wie ein Netzwerkadaptergerät oder auch eine Sammlung von Komponenten wie zum Beispiel ein Computer (das Computerobjekt könnte auch das Netzwerkadapterobjekt enthalten) sein. So genannte Provider müssen die Darstellung des Objekts definieren und bereitstellen, auf das die Managementanwendungen zugreifen sollen. Wenn zum Beispiel ein Lieferant eines Netzwerkadapters seinen Adapter WMI-fähig machen will, muss er einen Provider entwickeln, der als Schnittstelle zum Adapter fungiert und bei Anforderungen durch Managementanwendungen den Status und die Funktionsweise von Attributen abfragt oder definiert. In einigen Fällen (z.B. Gerätetreiber) liefert Microsoft einen Provider mit eigenem API, um Entwickler von Provider-Plug-ins, die die Implementierung des Providers nutzen, durch eine Minimierung des Codieraufwands zu unterstützen.

Die WMI-Infrastruktur verbindet die Managementanwendungen und die Provider miteinander. Die Infrastruktur dient zudem als Objektklassenspeicher und in vielen Fällen auch als Speichermanager für dauerhafte Objekteigenschaften. WMI implementiert das Repository als eine Datenbank auf dem Datenträger. Im Rahmen der Infrastruktur unterstützt WMI mehrere APIs, mit deren Hilfe Managementanwendungen auf Objektdaten zugreifen können, wobei die Provider Daten und Klassendefinitionen bereitstellen.

Win32-Programme nutzen das WMI-COM-API, das primäre Management-API, zur direkten Interaktion mit WMI. Andere APIs bilden Schichten über dem COM-API und enthalten auch einen ODBC-Adapter für Microsoft Access. Ein Datenbankentwickler verwendet den WMI-ODBC-Adapter, um Verweise auf Objektdaten in der Datenbank des Entwicklers einzubetten. Dieses Verfahren gibt ihm die Möglichkeit, auf einfache Weise Berichte mit Datenbankabfragen zu generieren, die WMI-basierte Daten enthalten. Die ActiveX-Steuerelemente von WMI unterstützen eine weitere API-Schicht. Web-Entwickler arbeiten mit den ActiveX-Steuerelementen, um Web-basierte Schnittstellen zu WMI-Daten aufzubauen. Ein weiteres Management-API ist das WMI-Skript-API, auf das in skriptgestützten Anwendungen und Visual-Basic-(VB-)Programmen zurückgegriffen werden kann. Eine WMI-Skriptunterstützung gibt es für VBScript, JScript, Active Server Pages (ASP) und HTML.

Bild 2. *Vererbung im Klassen-Browser CIM Studio*

Ebenso wie für Managementanwendungen bilden WMI-COM-Schnittstellen das primäre API für Provider. Im Unterschied zu Managementanwendungen, die COM-Clients darstellen, sind die Provider COM- oder DCOM-(Distributed-COM-)Server, d.h., die Provider implementieren COM-Objekte, mit denen WMI interagiert. Ein WMI-Provider kann auf DLLs zurückgreifen, die in den Verwaltungsprozess von WMI geladen werden sowie auf eigenständige Win32-Anwendungen oder Win32-Dienste. Microsoft liefert eine Anzahl integrierter Provider mit, die Daten aus bekannten Quellen wie dem Performance-API, der Registrierung und dem Ereignismanager bereitstellen. Das WMI-Software-Development-Kit (SDK) ermöglicht Entwicklern die Erstellung eigener WMI-Provider.

Provider Das Kernstück von WBEM ist die Spezifikation der Art und Weise, wie Managementsysteme aus Sicht des Systemmanagements die einzelnen Elemente, angefangen beim Computer bis hin zu einer Anwendung oder einem Teil in einem Computer, darstellen. Diese Spezifikation, die als Common Information Model (CIM) bezeichnet wird, wurde von der DMTF entwickelt. Entwickler von Providern verwenden CIM, um die Komponenten einer Anwendung darzustellen, für die die Entwickler Managementfunktionen implementieren wollen. Zur Implementierung einer CIM-Darstellung dient die MOF-(Managed-Object-Format-)Sprache.

Neben der Definition von Objekten muss ein Provider auch eine WMI-Schnittstelle zu den Objekten bieten. WMI klassifiziert die Provider nach den Schnittstellenfunktionen, die von den Providern bereitgestellt werden. In der Tabelle „Provider-Klassifizierungen“ sind Provider-Klassifizierungen von WMI aufgelistet. Zu beachten ist, dass ein Provider eine oder mehrere Funktionen implementieren kann. Daher kann ein Provider zum Beispiel gleichzeitig als Klassen- und als Ereignis-Provider auftreten. Zur Verdeutlichung der Funktionsdefinitionen soll kurz das Beispiel eines Providers beschrieben werden, der die meisten dieser Funktionen implementiert. Der Event Log Provider definiert verschiedene Objekte, zu denen die Objekte „Event Log Computer“, „Event Log Record“ und „Event Log File“ gehören. Der Provider „Event Log“ ist ein Klassen-Provider, da er diese Objekte mit Hilfe von Klassen definiert und diese Klassendefinitionen an WMI weitergeben muss. Außerdem ist dieser Provider ein Instanz-Provider, weil er mehrere Instanzen für unterschiedliche Klassen definieren kann. Eine Klasse, für die der Provider „Event Log“ mehrere Instanzen definiert, ist die Klasse „Event Log File“. Er definiert eine Instanz für jedes der Ereignisprotokolle des Systems (d.h. Systemereignisprotokoll, Anwendungsereignisprotokoll und Sicherheitsereignisprotokoll).

Der Provider „Event Log“ definiert die Instanzdaten und gibt Managementanwendungen die Möglichkeit, die Datensätze zu durchsuchen. Dieser Provider ermöglicht es einer Managementanwendung außerdem, die Eigenschaften bestimmter Ereignisprotokolldatensätze abzufragen. Diese Möglichkeit klassifiziert den Provider „Event Log“ als Eigenschafts-Provider. Damit Managementanwendungen mit Hilfe von WMI Ereignisprotokolldateien sichern und wiederherstellen können, implementiert der Provider Sicherungs- und Wiederherstellungsmethoden für Objekte der Klasse „Event Log File“. Dadurch wird er zu einem Methoden-Provider. Und schließlich kann sich eine Managementanwendung registrieren, um eine Benachrichtigung zu erhalten, wenn ein neuer Datensatz in eines der Ereignisprotokolle geschrieben wird. Auf diese Weise dient der Provider „Event Log“ als Ereignis-Provider, wenn er mit Hilfe der WMI-Ereignisbenachrichtigung WMI mitteilt, dass Datensätze für ein Ereignisprotokoll eingetroffen sind.

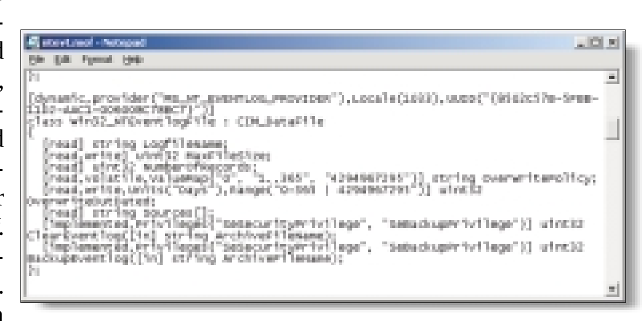


Bild 3. *Definieren von Win32_NTEventlogFile*

CIM und MOF CIM tritt in die Fußstapfen objektorientierter Sprachen wie C++ und Java, in denen ein Modelldesigner Darstellungen in Form von Klassen entwirft. Mit Hilfe der Klassen können Entwickler sich die leistungsstarken Modelliertechniken der Vererbung und Composition zunutze machen. Unterklassen können die Attribute einer anderen Klasse „erben“ und ihnen anschließend eigene Merkmale zuweisen oder die Merkmale, die sie von der übergeordneten Klasse erhalten, außer Kraft setzen. Eine Klasse, die Eigenschaften aus einer anderen Klasse übernimmt, wird aus der übergeordneten Klasse „abgeleitet“. Darüber hinaus können Klassen auch zusammengesetzt werden: Ein Entwickler kann eine Klasse erstellen, die wiederum andere Klassen enthält.

Die DMTF stellt mehrere Klassen als Teil des WBEM-Standards bereit. Diese Klassen bilden die Grundelemente von CIM und stellen Objekte dar, die auf alle Bereiche des Managements angewandt werden können. Die Klassen sind Teil des CIM-Kernmodells. Ein Beispiel einer Kernklasse ist CIM_ManagedSystemElement. Diese Klasse enthält einige Grundeigenschaften, die physische Komponenten wie Hardware-Geräte und logische Komponenten wie Prozesse und Dateien kennzeichnen. Zu den Eigenschaften gehören eine Kennung, eine

Beschreibung, das Installationsdatum und der Status. Die Klassen CIM_LogicalElement und CIM_PhysicalElement übernehmen nun die Attribute der Klasse CIM_ManagedSystemElement. Diese beiden Klassen gehören ebenfalls zum CIM-Kernmodell. Der WBEM-Standard bezeichnet diese Klassen als abstrakte Klassen, weil sie ausschließlich als Klassen vorhanden sind, deren Attribute von anderen Klassen übernommen werden (d.h., es gibt keine Instanzen einer abstrakten Klasse). Eine abstrakte Klasse könnte also als Schablone aufgefasst werden, die Eigenschaften zur Verwendung in anderen Klassen definiert.

Eine zweite Kategorie von Klassen stellt Objekte dar, die für Managementbereiche spezifisch, jedoch nicht von einer bestimmten Implementierung abhängig sind. Diese Klassen bilden das Common Model und werden als Erweiterung des Kernmodells betrachtet. Ein Beispiel einer Klasse des allgemeinen Modells ist die Klasse CIM_FileSystem, die die Attribute der Klasse CIM_LogicalElement übernimmt. Da praktisch jedes Betriebssystem, einschließlich Win2K, Linux und andere Varianten von Unix, mit einem in Form eines Dateisystems strukturierten Speicher arbeitet, ist die Klasse CIM_FileSystem ein zweckdienlicher Bestandteil des Common Modells.

Die letzte Klassenkategorie umfasst technologiespezifische Erweiterungen zur allgemeinen Klasse. Win2K definiert einen umfangreichen Satz dieser Klassen, um für die Win32-Umgebung spezifische Objekte darzustellen. Da alle Betriebssysteme Daten in Dateien speichern, enthält das allgemeine CIM-Modell die Klasse CIM_LogicalFile. Die Klasse CIM_DataFile beerbt die Klasse CIM_LogicalFile, und Win32 fügt die Dateiklassen Win32_PageFile und Win32_ShortCutFile für diese Win32-Dateiarten hinzu.

Der Provider „Event Log“ nutzt die Möglichkeiten der Vererbung weidlich aus. Bild 2 enthält ein Screenshot von WMI CIM Studio, einem Klassen-Browser, der mit dem WMI SDK geliefert wird. (Microsoft liefert das WMI SDK im Rahmen des Microsoft Developer Networks – MSDN aus.) Es ist zu erkennen, wo der Provider „Event Log“ auf die Vererbung in der Klasse Win32_NTEventlogFile des Providers zurückgreift, die aus der Klasse CIM_DataFile abgeleitet ist. Ereignisprotokolldateien sind Datendateien, die zusätzliche für das Ereignisprotokoll spezifische Attribute wie einen Protokolldateinamen und die Anzahl der in der Datei enthaltenen Datensätze besitzt. Die Baumstruktur, die vom Klassen-Browser angezeigt wird, offenbart, dass sich die Klasse Win32_NTEventlogFile auf mehrere Ebenen der Vererbung stützt, in denen die Klasse CIM_DataFile aus der Klasse CIM_LogicalElement und die Klasse CIM_LogicalElement wiederum aus der Klasse CIM_ManagedSystemElement abgeleitet ist.

Wie bereits zuvor erwähnt, schreiben Entwickler von WMI-Klassen-Providern ihre Klassen in MOF. Bild 3 zeigt die Definition der Klasse Win32_NTEventlogFile des Providers „Event Log“, die in Bild 2 hervorgehoben ist. Zu beachten ist die Korrelation zwischen den sechs Eigenschaften im oberen Bereich des rechten Fensters in Bild 2 und den Eigenschaften dieser Definitionen in der MOF-Datei in Bild 3. CIM Studio verwendet gelbe Pfeile, um diejenigen Eigenschaften zu markieren, die eine Klasse übernimmt, weshalb diese Eigenschaften nicht in der Definition der Klasse Win32_NTEventlogFile aufgeführt werden.

Eine Bezeichnung, die näher unter die Lupe genommen werden sollte, ist der Bezeichner „dynamisch“, mit dem die Klasse Win32_NTEventlogFile beschrieben wird, die in der MOF-Datei in Bild 3 zu sehen ist. Diese Bezeichnung gibt an, dass die WMI-Infrastruktur die Werte von Eigenschaften, die mit einer Klasse verbunden sind, jedes Mal aus dem WMI-Provider abruft, wenn eine Managementanwendung die Eigenschaften abfragt. Demgegenüber ist eine statische Klasse eine Klasse, deren Eigenschaften vom Provider im WMI-Repository gespeichert werden. Die WMI-Infrastruktur greift auf dieses Repository zu, um

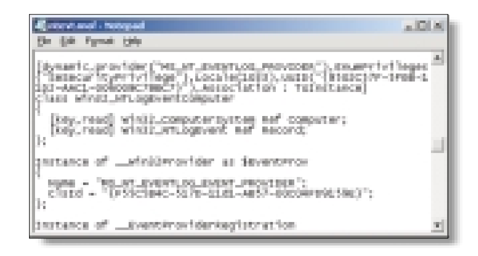


Bild 4. *Abb.n einer Klassenzuordnung*

die Werte abzurufen, anstatt die Daten vom Provider anzufordern. Da das Aktualisieren des WMI-Speichers eine relativ aufwendige Operation ist, sind dynamische Provider für solche Objekte effizienter, die durch häufige Änderungen gekennzeichnete Eigenschaften besitzen.

Nach dem Aufbau von Klassen in MOF können WMI-Entwickler die Klassendefinitionen auf verschiedene Arten an WMI weitergeben. Eine Möglichkeit ist die, eine MOF-Datei im BMF-Format (Binary MOF Format – eine kompaktere Binärdarstellung als MOF) zu kompilieren und die BMF-Dateien an die WMI-Infrastruktur zu übergeben. Eine andere Methode besteht darin, dass der Provider MOF-Definitionen kompiliert und mit Hilfe von WMI-COM-APIs an die WMI-Infrastruktur übergibt. Und schließlich kann ein Provider mit Hilfe des Tools Mofcomp eine kompilierte Klassendarstellung an die WMI-Infrastruktur direkt übergeben.

WMI Namespace Klassen definieren die Eigenschaften von Objekten, während Instanzen von Klassen Objekte in einem System darstellen. WMI verwendet einen Namensraum (Namespace), der verschiedene Unternamensräume enthält, die von WMI zur Organisation von Objektinstanzen hierarchisch angeordnet werden. Eine Managementanwendung muss zunächst eine Verbindung zu einem Namensraum herstellen, bevor sie auf Objekte innerhalb des Namensraums zugreifen kann. WMI bezeichnet den Ursprung des Namensraums als Root. Alle WMI-Installationen besitzen vier vordefinierte Namensräume, die sich unterhalb des Roots befinden: CIMV2, Default-Verzeichnis, Security und WMI. Einige dieser Namensräume wie zum Beispiel CIMV2 enthalten selbst weitere Namensräume. Zum Beispiel enthält CIMV2 die Namensräume Applications und ms_409 als Unternamensräume. Provider definieren zuweilen eigene Namensräume. In Win2K ist der WMI-Namensraum (der von dem WMI-Provider für Windows-Gerätetreiber definiert wird) unterhalb des Roots zu sehen.

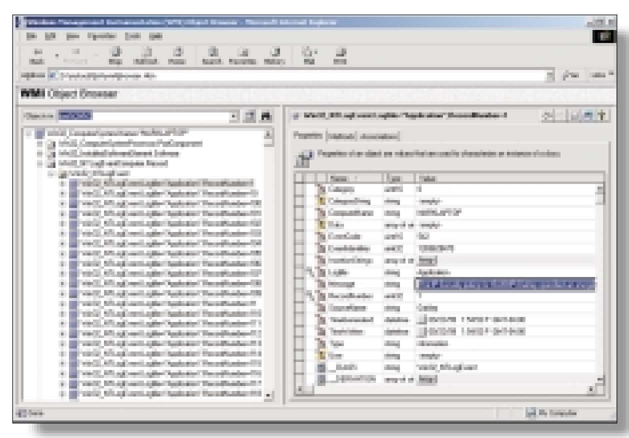


Bild 5. *Abb.n eines Namensraumstamms mit Object Browser*

Im Unterschied zum Namensraum eines Dateisystems, der eine Hierarchie von Verzeichnissen und Dateien enthält, besitzt ein WMI-Namensraum nur eine Ebene. Statt Namen wie ein Dateisystem zu verwenden, arbeitet WMI mit Objekteigenschaften, die als Schlüssel zur Bezeichnung von Objekten definiert werden. Managementanwendungen geben Klassennamen mit Schlüsselnamen an, um bestimmte Objekte innerhalb eines Namensraums ausfindig zu machen. Dies bedeutet, dass jede Instanz einer Klasse durch ihre Schlüsselwerte eindeutig identifizierbar sein muss. Zum Beispiel verwendet der Provider „Event Log“ die Klasse Win32_NTLogEvent, um einen Eintrag in einem Ereignisprotokoll darzustellen. Diese Klasse besitzt zwei Schlüssel: LogFile und RecordNumber. Beide Schlüssel sind Zeichenfolgen. Eine Managementanwendung, die WMI nach Instanzen von Ereignisprotokolleinträgen abfragt, erhält vom Provider Schlüsselpaare, die Datensätze angeben. Anschließend kann die Anwendung mit einer Syntax auf einen Datensatz zugreifen, die durch das folgende Beispiel eines Objektspfadnamens veranschaulicht wird: \\MARKLAPTOP\CIMV2:Win32_NTLogEvent.Logfile=„Application“,RecordNumber=„1“. Die erste Komponente in dem Namen gibt den Computer an, auf dem sich das Objekt befindet. Die zweite Komponente bezeichnet den Namensraum des Objekts. Der Klassenname folgt auf den Doppelpunkt, die Schlüsselnamen und ihre zugehörigen Werte stehen nach dem Punkt. Ein Komma trennt die einzelnen Schlüsselwerte.

Klassenzuordnung Viele Objekttypen stehen in einer bestimmten Beziehung zueinander. Zum Beispiel besitzt ein Computerobjekt einen Prozessor, installierte Software, ein Betriebssystem, aktive Prozesse usw. WMI ermöglicht

Providern, eine Zuordnungsklasse zu konstruieren, um eine logische Verbindung zwischen zwei verschiedenen Klassen darzustellen. Zuordnungsklassen ordnen eine Klasse einer anderen zu, sodass die Klassen nur zwei Eigenschaften besitzen. Da die Eigenschaften Verweise auf Klassen sind, bestehen sie aus einem Klassennamen und der Referenzangabe (Ref). In Bild 4 ist eine Zuordnung zu sehen, in der die MOF-Datei des Providers „Event Log“ die Klasse Win32_NTLogEvent der Klasse Win32_ComputerSystem zuordnet. Für ein gegebenes Objekt kann eine Managementanwendung zugeordnete Objekte abfragen. Auf diese Weise kann ein Provider eine Hierarchie von Objekten definieren.

Bild 5 zeigt den WMI Object Browser (ein weiteres Entwicklungsprogramm, das im WMI SDK enthalten ist), der den Stamm (Root) des Namensraums CIMV2 anzeigt. Win32-Systemkomponenten legen ihre Objekte in der Regel innerhalb des Namensraums CIMV2 an. Der Objekt-Browser beginnt, indem er die Instanz „MARKLAPTOP“ des Objekts Win32_ComputerSystem lokalisiert, also das Objekt, das den Computer darstellt. Dann ruft der Objekt-Browser die der Klasse Win32_ComputerSystem zugeordneten Objekte ab und zeigt sie unter MARKLAPTOP an. Die Benutzerschnittstelle von Object Browser stellt Zuordnungsobjekte mit einem Doppelpfeilordnersymbol dar. Die Objekte des Typs der Zuordnungsklasse werden unterhalb des Ordners angezeigt.

Im Objekt-Browser ist zu erkennen, dass die Zuordnungsklasse Win32_NTLogEventComputer des Providers „Event Log“ unterhalb von MARKLAPTOP dargestellt wird, und dass zahlreiche Instanzen der Klasse Win32_NTLogEvent vorhanden sind. Bild 4 ist zu entnehmen, dass die MOF-Datei die Klasse Win32_NTLogEventComputer definiert, um der Klasse Win32_ComputerSystem die Klasse Win32_NTLogEvent zuzuordnen. Das Anklicken einer Instanz von Win32_NTLogEvent im Objekt-Browser zeigt die Eigenschaften dieser Klasse im rechten Fensterbereich an. Microsoft beabsichtigte, mit dem Programm Object Browser WMI-Entwickler bei der Untersuchung ihrer Objekte zu unterstützen, jedoch würde eine Managementanwendung wohl die gleichen Operationen ausführen und Eigenschaften bzw. gesammelte Daten in etwas verständlicher Form präsentieren.

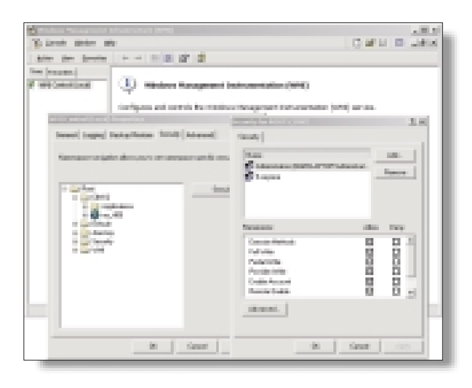


Bild 6. *Konfigurieren der Namensraumsicherheit*

Implementierung von WMI

Die WMI-Infrastruktur wird in der Hauptsache durch die ausführbare Datei \winnt\system32\wbem\winmgmt.exe implementiert. Diese Datei wird als Win32-Dienst ausgeführt, der vom Win2K-Dienstemanager (Service-Control-Manager) gestartet wird, wenn eine Managementanwendung oder ein WMI-Provider zum ersten Mal versucht, auf WMI-APIs zuzugreifen. Die meisten WMI-Komponenten befinden sich in den Verzeichnissen \winnt\system32 und \winnt\system32\wbem, einschließlich der Win32-MOF-Dateien, der integrierten Provider-DLLs und der WMI-DLLs für Managementanwendungen. Zum Beispiel zeigt ein Blick in das Verzeichnis \winnt\system32\wbem, dass sich dort die Datei ntevt.mof befindet, die MOF-Datei für den Provider „Event Log“. Außerdem findet sich hier die Datei ntevt.dll, die DLL des Providers „Event Log“, die von winmgmnt.exe geladen wird.

In Verzeichnissen unter \winnt\system32\wbem werden der WIM-Speicher (Repository), Protokolldateien und MOF-Dateien von Drittherstellern untergebracht. WMI implementiert das Repository, das als CIM Object Management-(CIMOM-)Repository bezeichnet wird, in Form der Datei \winnt\system32\wbem\repository\cim.rep. WinMgmt berücksichtigt zahlreiche Registrierungseinstellungen, die sich auf das Repository beziehen (einschließlich verschiedener interner leistungsrelevanter Parameter wie CIMOM-Sicherungsspeicherpositionen und Sicherungsintervalle), die im Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM gespeichert werden.

Microsoft wollte die Managementfunktionalität auf alle Aspekte von Win2K ausdehnen, sodass eine Möglichkeit für Gerätetreiber zur Interaktion mit WMI geschaffen werden musste. Gerätetreiber verwenden verschiedene neue Schnittstellen, um Daten bereitzustellen und Befehle von WMI entgegenzunehmen. Die WMI-Befehle werden von Microsoft als Systemsteuerbefehle (System Control commands) bezeichnet. Microsoft gab dem Gerätetreiber-Provider den Namen Windows-Driver-Model-(WDM-) Provider, weil die gleichen WMI-Schnittstellen in Win2K-Treibern für Win98-Treiber vorhanden sind. Da die Schnittstellen plattformübergreifend arbeiten, fallen sie unter WDM, die plattformübergreifende Gerätetreiberarchitektur. Unter Win2K werden WDM-Objekte im Namensraum \root\wmi gespeichert.

WMI-Sicherheit

WMI implementiert Sicherheit auf der Namespace-Ebene. Wenn eine Managementanwendung erfolgreich eine Verbindung zu einem Namensraum herstellt, kann die Anwendung die Eigenschaften aller Objekte in diesem Namensraum anzeigen und auf sie zugreifen. Mit Hilfe der Anwendung WMI Control kann ein Administrator steuern, welche Benutzer auf einen Namensraum zugreifen können. Zum Starten der WMI-Steueranwendung muss im Menü „Start“ die Option „Verwaltung“ und dann „Computerverwaltung“ ausgewählt werden. Als Nächstes muss die Verzweigung für Dienste und Anwendungen geöffnet werden. Durch Klicken mit der rechten Maustaste auf WMI und Auswählen der Option für Eigenschaften wird das Dialogfeld für die (lokalen) WMI-Steuereigenschaften geöffnet, das in Bild 6 zu sehen ist. Zur Konfiguration von Sicherheit für Namensräume auf der Registerkarte für Sicherheit muss der Namensraum hervorgehoben und anschließend „Sicherheit“ gewählt werden. Andere Registerkarten im Dialogfeld ermöglichen ein Ändern der Leistungs- und Sicherungseinstellungen, die in der Registrierung gespeichert werden.

In dem hier zur Verfügung stehenden Rahmen konnten das umfangreiche Thema WMI und viele Aspekte der reichhaltigen WMI-Funktionalität nur angeschnitten werden. Die Flexibilität und universelle Anwendung auf alle möglichen Komponenten von Win2K machen WMI zu einer leistungsstarken Middleware-Technologie, deren Vorteile in Zukunft ohne Zweifel von Unternehmensprogrammentwicklern erkannt und zur Schaffung mächtiger Dienstprogramme für das Unternehmensmanagement genutzt werden. (kl)

Grundlagen und Tipps zu NT-Domänen-Controllern

Meine Domäne, mein PDC, mein BDC!

von L. J. Locher

Domänen sind ein grundlegendes Konzept von Windows-NT-Netzwerken. Sie sind der Gültigkeitsbereich für Benutzerkosten, Rechnernamen und gemeinsame Sicherheitsrichtlinien. Im Zentrum jeder NT-Domäne stehen die Verwaltungs- und Anmelde-Server, die so genannten Domänen-Controller. Dieser Artikel erklärt, was primäre und Sicherungs-Domänen-Controller ausmacht und gibt Tipps zur richtigen Verwaltung.

Windows NT Server organisiert Computergruppen in Domänen, sodass alle Maschinen in einer Domäne eine gemeinsame Datenbank und eine Sicherheitsrichtlinie benutzen können. Domänen-Controller sind Rechner, auf denen NT Server aktiv ist und die eine zentralisierte Verzeichnisdatenbank gemeinsam verwenden, in der Benutzerkonten- und Sicherheitsinformationen für eine Domäne gespeichert werden. Wenn sich Benutzer an einem Domänenkonto anmelden, authentifizieren die Domänen-Controller den Benutzernamen und das Kennwort des Benutzers anhand der Informationen in der Verzeichnisdatenbank. Die Verzeichnisdatenbank wird mitunter als Sicherheitsdatenbank der Domäne oder als SAM-Datenbank bezeichnet. Während der Installation von NT Server muss die Funktion, die Server in einer Domäne ausüben sollen, festgelegt werden. In NT gibt es für diese Funktion drei Auswahlmöglichkeiten: Primärer Domänen-Controller (PDC), Backup-Domänen-Controller (BDC) und Mitglieds-Server (oder eigenständiger Server). Eine Domäne wird erstellt, wenn der Benutzer einen PDC festlegt. PDCs und BDCs sind entscheidende Elemente in der Domänentheorie und der Domänenpraxis. Zur Implementierung der Steuerung von Domänen, die in einem NT-Netzwerk eingerichtet werden, und zur optimalen Verwendung dieser Domänen sind Kenntnisse darüber erforderlich, was PDCs und BDCs sind, wie die Verzeichnisdatenbank auf einem PDC mit den Kopien der Datenbank auf den BDCs in den zugehörigen Domänen synchronisiert wird, wie ein BDC zu einem PDC höhergestuft wird, wenn der PDC offline ist, wie die optimale Anzahl von BDCs für eine Domäne ermittelt wird und wie Beziehung zwischen den PDCs getrennter Domänen verwaltet wird.

PDCs und BDCs: Was ist der Unterschied? Obwohl NT-4.0- und NT-3.51-Domänen mehrere Server enthalten können, kann nur ein Server in der Domäne ein primärer Domänen-Controller (PDC) sein. Der PDC speichert Domänenkonten und Sicherheitsinformationen in der Master Copy der Verzeichnisdatenbank, die vom PDC gepflegt wird. Wenn von Benutzern Änderungen an Benutzerkonten oder Sicherheitsinformationen vorgenommen werden, zeichnet der PDC die Änderungen in der Master Copy der Verzeichnisdatenbank auf. Ein PDC ist der einzige Domänen-Server, der diese Änderungen direkt empfängt. Mit anderen Worten,

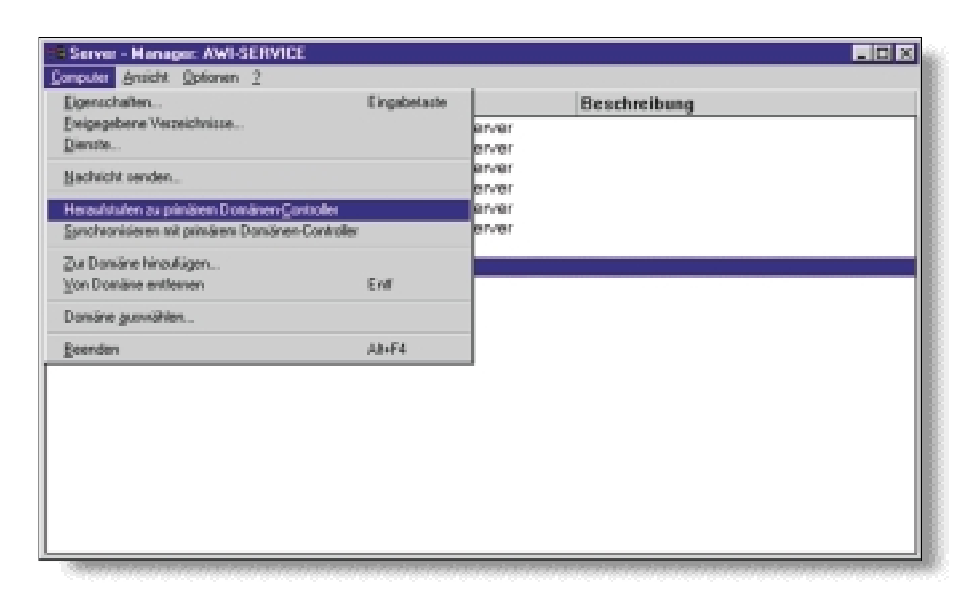


Bild 1. *Heraufstufen eines BDC zu einem PDC im Server-Manager*

PDCs speichern eine Schreib-/Lesekopie der Verzeichnisdatenbank.

Eine Domäne kann über mehrere Backup-Domänen-Controller (BDC) verfügen. Jeder BDC in einer Domäne unterhält eine reine Lesekopie der Hauptverzeichnisdatenbank des PDC. An der Kopie der Verzeichnisdatenbank auf dem BDC können keine Änderungen durchgeführt werden. Da zwischen der Hauptverzeichnisdatenbank auf dem PDC und den Verzeichnisdatenbankkopien auf den BDCs eine Duplizierung der Verzeichnisdatenbank stattfindet, kann jeder BDC in einer Domäne zum PDC höhergestuft werden, wenn der ursprüngliche PDC ausfällt oder zu Wartungszwecken heruntergefahren werden muss. BDCs unterstützen zudem eine Verteilung der Arbeitslast, die durch die Authentifizierung von Netzwerkanmeldungen entsteht.

Von entscheidender Bedeutung ist der Betrieb wenigstens eines BDC in einer Domäne. Falls der PDC ausfällt, kann die Domäne funktionsfähig gehalten werden, indem der BDC in einen PDC umgewandelt wird. Diese Heraufstufung des BDC gewährleistet, dass Änderungen an der Verzeichnisdatenbank durchgeführt werden können und diese Änderungen im gesamten Netzwerk verbreitet werden. Die Höherstufung eines BDC garantiert zudem den Zugriff auf Netzwerkressourcen und sorgt dafür, dass die Verzeichnisdatenbank für die Domäne zugänglich bleibt. Wenn die Verzeichnisdatenbank für die Domäne nicht zugänglich ist, können Benutzer nicht angemeldet und in der Domäne nicht authentifiziert werden. Computer können sich nicht selbst der Domäne gegenüber identifizieren und können daher auch keinen sicheren Kanal herstellen, der für die Kommunikation zwischen den Rechnern in der Domäne erforderlich ist. Gruppenkonten haben keinen Zugriff auf Ressourcen in der Domäne. Kurz, ohne BDC, der zu einem PDC heraufgestuft werden kann, geraten Administratoren im Falle eines PDC-Ausfalls in arge Verlegenheit, weil der Zugriff auf das gesamte Netzwerk unterbrochen wird.

Ähnlich wie bei NT speichern Domänen-Controller unter Windows 2000 (Win2K) eine Kopie der Verzeichnisdatenbank. Im Unterschied zu NT 4.0 und NT 3.51, bei denen ein Replikationsmodell mit einer Hauptkopie (Single Master Replication Model) implementiert wird, in dem nur der PDC einer Domäne die Hauptkopie der Verzeichnisdatenbank enthält, unterhalten sämtliche Win2K-Domänen-Controller eine Schreib-/Lesekopie der Verzeichnisdatenbank. Außerdem muss unter NT 4.0 und NT 3.51 der PDC einer Domäne stets zugänglich sein, damit Änderungen an der Verzeichnisdatenbank ausgeführt werden können. Dies ist bei Win2K nicht der Fall, weil durch Active Directory (AD) ein Multimaster-Replikationsmodell (d.h. ein Modell mit mehreren Hauptkopien der Verzeichnisdatenbank) implementiert wird. Dieses Replikationsmodell ermöglicht Administratoren, Änderungen an der Verzeichnisdatenbank auf einem beliebigen Domänen-Controller in einer Domäne vorzunehmen. Der Domänen-Controller repliziert anschließend die Änderungen auf alle anderen Domänen-Controller in der Domäne. Das Ergebnis ist eine 100-prozentige Verfügbarkeit der Verzeichnisdatenbank, selbst wenn einzelne Domänen-Controller zeitweilig nicht verfügbar sind. Alle Domänen-Controller im Multimaster-Replikationsmodell sind gleichberechtigt. Das heißt, es gibt keine Unterscheidung in PDCs und BDCs. Im Kasten „Migration zu einer Windows 2000-Domäne von einer NT 4.0- oder NT 3.51-Domäne“ wird erläutert, was mit den Domänen-Controllern bei der Migration auf Win2K geschieht.

Synchronisierung von Domänen-Controllern Eine Replikation der Verzeichnisdatenbank findet statt, wenn der PDC einer Domäne die Datenbank mit jedem BDC in der eigenen Domäne synchronisiert. Das System synchronisiert alle BDCs einer Domäne regelmäßig, um die zentrale Sicherheit aufrecht zu erhalten. Nach der Erstkonfiguration eines BDC wird eine vollständige Synchronisierung mit dem PDC durchgeführt. Daher ist es vorteilhaft, die Verbindung über eine Hochgeschwindigkeitsverbindung einzurichten. Nach dieser vollständigen Synchronisierung finden Teilsynchronisierungen statt, wenn von einem Benutzer oder vom System Änderungen an der Verzeichnisdatenbank des PDC vorgenommen werden.

Gelegentlich kann die Synchronisierung der Verzeichnisdatenbank der Domäne auf einem BDC nicht korrekt durchgeführt werden. Zum Beispiel könnte der BDC ausfallen oder es könnten Zeitlimitprobleme während der Netzwerkkommunikation auftreten. Wenn die Synchronisierung eines BDC nicht mehr korrekt ist, kann eine manuelle Synchronisierung durchgeführt werden. In NT 3.51 konnte eine vollständige Synchronisierung eines bestimmten BDC durch Auswählen der Option zum Synchronisieren mit primärem Domänen-Controller im Menü „Computer“ des Server-Managers eingeleitet werden. Die gleiche Auswahl in NT 4.0 bewirkt indes nur eine Teilsynchronisierung, wenn sowohl der PDC als auch der BDC unter NT Server 4.0 betrieben werden (siehe Kasten „Domänenverwaltung von einer NT-Workstation“, falls Informationen zur Verwaltung von Domänen über eine NT-Workstation erwünscht sind). Aus diesem Grund muss eine vollständige Synchronisierung durch Ausführen des Befehls Net accounts/synch über eine Eingabeaufforderung auf dem nicht synchronisierten BDC erzwungen werden. Eine manuelle Synchronisierung aller Domänen-Controller in einer Domäne kann durch Auswählen des PDC der Domäne im Server-Manager und der Option „Synchronisieren der gesamten Domäne“ im Menü „Computer“ durchgeführt werden.

Tipp: So viele PDCs brauchen Sie

Anzahl Benutzerkonten	Anzahl BDCs
Unter 5000	1
5000	2
10.000	5
20.000	10
30.000	15

Höherstufen von Domänen-Controllern Zuweilen muss ein BDC zu einem PDC höhergestuft werden. Beispielsweise könnte eine Routinewartung am PDC erforderlich werden oder Hardware-Probleme auf dem PDC auftreten. Wenn ein BDC zu einem PDC heraufgestuft wird, stuft das System automatisch den ursprünglichen PDC zu einem BDC herab, nachdem eine Replikation stattgefunden hat.

Zur Heraufstufung eines BDC zu einem PDC wird im Server-Manager der

gewünschte Sicherungs-Domänen-Controller ausgewählt. Im Menü „Computer“ muss anschließend die Option „Heraufstufen zu primärem Domänen-Controller“ ausgewählt werden wie in Bild 1 zu sehen ist. Falls der Server-Manager den PDC nicht auffinden kann, wird eine Meldung mit einem entsprechenden Hinweis angezeigt. Der Server-Manager bietet die Möglichkeit, fortzufahren, ohne den PDC herabzustufen bzw. zu warten, bis der Server-Manager den PDC finden und herabstufen kann.

Heraufstufen eines BDC bei nicht verfügbarem PDC: Im Allgemeinen kann eine Domäne für eine kurze Zeit ohne den zugehörigen PDC funktionieren. Allerdings ist das Offline-Setzen eines PDC für einen längeren Zeitraum als eine Stunde, ohne einen BDC ersatzweise heraufzustufen, keine gute Verfahrensweise. Wenn ein PDC länger als eine Stunde außer Betrieb genommen werden muss bzw. wenn der PDC abstürzt, können keine Änderungen an Benutzerkonten und Sicherheitsrichtlinien implementiert werden, während der PDC nicht zur Verfügung steht. Die Domäne authentifiziert unterdessen weiterhin Benutzer, die sich immer noch an der Domäne anmelden können.

Wenn ein BDC heraufgestuft wird, während der PDC offline ist, zeigt der Server-Manager die Warnung an, dass der primäre Domänen-Controller für die Domäne nicht gefunden werden kann. Die Domäne kann verwaltet werden, aber bestimmte Befehlsoperationen werden deaktiviert. Es treten auch andere Schwierigkeiten auf, wenn ein BDC heraufgestuft wird, während der PDC offline ist. Wenn der ursprüngliche PDC wieder online verfügbar wird, hat ihn der Server-Manager vielleicht immer noch als PDC in seiner Liste, aber dies entspricht nicht mehr den Tatsachen. Erkennt der ursprüngliche PDC den PDC, der von einem BDC heraufgestuft wurde, schließt der ursprüngliche PDC seine Dienste zur Netzwerkanmeldung und Remote-Management, blendet sein Symbol im Server-Manager aus und nimmt nicht mehr an der Authentifizierung von Benutzeranmeldungen oder der Synchronisierung mit dem aktuellen PDC teil. Wenn dies geschieht, stellt der ursprüngliche PDC kaum mehr als eine NT-Workstation dar.

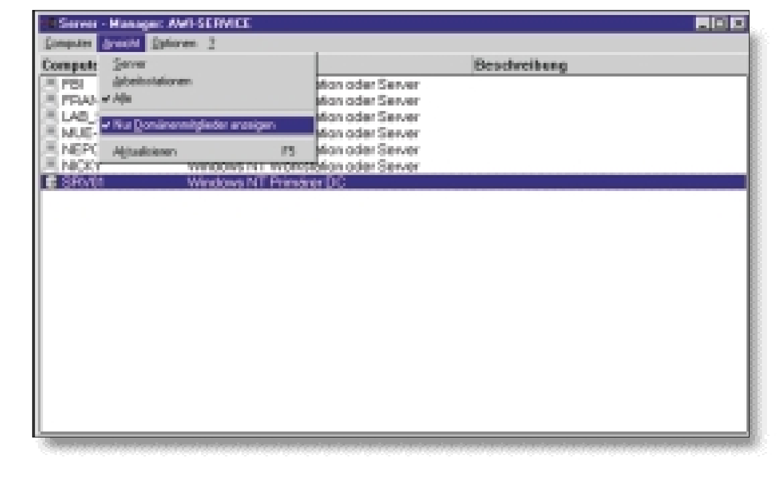


Bild 2. *Deaktivieren des Eintrags „Nur Domänenmitglieder anzeigen“*

Soll der ursprüngliche PDC in seine Rolle als PDC wieder eingesetzt werden, muss er zunächst zu einem BDC herabgestuft und eine Synchronisierung mit dem Ersatz-PDC durchgeführt werden. Geschieht dies nicht, können alle Änderungen, die von Benutzern oder dem System am Ersatz-PDC vorgenommen wurden, einschließlich Änderungen an den Geheimnissen der lokalen Local Security Authority (SLA), nicht mit dem ursprünglichen PDC synchronisiert werden. Infolgedessen würden die an dem Ersatz-PDC vorgenommenen Änderungen verloren gehen. Aus diesem Grund muss der ursprüngliche PDC zur Wiedereinsetzung in seine Funktion als PDC zu einem BDC herabgestuft, die Synchronisierung mit dem Ersatz-PDC durchgeführt und anschließend der vom PDC herabgestufte BDC wieder zu einem PDC höhergestuft werden. Im Folgenden wird diese Heraufstufung im Einzelnen beschrieben.

Bei der Herabstufung des ursprünglichen PDC zu einem BDC ist zunächst sicherzustellen, dass der Eintrag „Nur Domänenmitglieder anzeigen“ des Menüs „Ansicht“ im Server-Manager deaktiviert wird wie in Bild 2 zu sehen ist. Die Funktion zum Durchsuchen informiert den Server-Manager, dass der ursprüngliche PDC als PDC konfiguriert ist und dass das System eine Herabstufung des PDC zu einem BDC zulässt. Wenn dieser Eintrag nicht deaktiviert wird, durchsucht der Server-Manager die Registrierung des aktuellen PDC, wodurch die Option zur Herabstufung des ursprünglichen PDC nicht zugelassen würde. Der aktuelle PDC würde den ursprünglichen PDC als BDC betrachten, da die Registrierung des aktuellen PDC die Rolle des ursprünglichen PDC in der Domäne nicht enthält. Die Rolle des aktuellen PDC ist die einzige Rolle als PDC, die das System kennt.

Zur Herabstufung des ursprünglichen PDC muss der Computername in der Suchliste des Server-Managers hervorgehoben und im Menü „Computer“ die Option „Herabstufen zu Sicherungs-Domänen-Controller“ ausgewählt werden. Anschließend muss die Option „Synchronisieren mit primärem Domänen-Controller“ ausgewählt werden, um diese Maschine mit dem aktuellen PDC zu synchronisieren. Schließlich muss die Option „Heraufstufen zu primärem Domänen-Controller“ ausgewählt werden, damit das System den aktuellen PDC herabstuft und den ursprünglichen PDC wieder höher stuft.

BDCs und Replikation Theoretisch ist die Anzahl der BDCs, die in einer Domäne vorhanden sein können, unbegrenzt. Aber die Anzahl der BDCs, die in einer Domäne eingerichtet werden können, unterliegt den Begrenzungen der realen Welt. Die Replikationszeit und der Replikationsverkehr sind zwei entscheidende Aspekte, durch die die optimale Anzahl von BDCs in einer bestimmten Domäne festgelegt wird.

Aufgrund seines Aufbaus begrenzt der Replikationsprozess den Bedarf an Netzwerkbandbreite. NT 3.51 versucht, bis zu zehn BDCs gleichzeitig zu replizieren. NT 4.0 versucht, bis zu 20 BDCs gleichzeitig zu replizieren. Technisch gesehen kann der Anmeldedienst zwischen 500 und 1000 BDCs in einer Domäne über eine schnelle Verbindung unterstützen. Langsamere Verbindungen (z.B. RAS, Modems mit 56 Kbps oder 128 Kbps) können bis zu 700 BDCs bewältigen. Jedoch ist der Betrieb einer großen Anzahl von BDCs in einer Domäne nicht sinnvoll, da die Begrenzung des Verkehrsvolumens unter einer großen Anzahl von BDCs verlangen würde, dass nur wenige

Verzeichnisänderungen gleichzeitig durchgeführt werden. Der optimale Aufbau einer Domäne verfügt über eine kleine Anzahl leistungsstarker Domänen-Controller, die über schnelle Netzwerkverbindungen miteinander verbunden sind. In Kasten „Tipp: ...“ werden die von Microsoft empfohlenen Verhältnisse zwischen Benutzerkonten und BDCs aufgeführt.

Probleme mit sicheren BDC-Kanälen Wenn der Anmeldedienst (Netlogon) unter NT Server 4.0 auf einem PDC gestartet wird, zählt das System alle Computerkonten in der Domäne auf und bildet eine Struktur, die einen sicheren Kanal zwischen dem PDC und den BDCs einrichtet. Der Anmeldedienst zählt eine Gruppe von 250 Konten bei jedem Aufruf an die Verzeichnisdatenbank auf. Aufgrund eines internen Fehlers lässt der Anmeldedienst innerhalb jeder 250er Gruppe ein Konto aus. Dieses Problem tritt nicht für Workstation-Konten auf. Allerdings kann das Problem bei BDC-Computerkonten auftreten, wenn der Anmeldedienst auf einem bestimmten BDC durch einen Fehler nicht startet.

Wenn der Anmeldedienst auf einem BDC nicht startet, zeichnet der BDC einen von zwei Fehlern des Anmeldedienstes auf: „Fehler 3210: Echtheitsbestätigung mit Computername, einem Windows NT-Domänen-Controller für Domäne Domänenname, fehlgeschlagen“ oder „Fehler 5721: Die Sitzung mit dem Windows NT-Domänen-Controller Unbekannt der Domäne Domänenname konnte nicht eingerichtet werden, da auf dem Windows NT Server kein Konto für den Computer Computername vorhanden ist.“ Der PDC kann eventuell ebenfalls einen von zwei Fehlern des Anmeldedienstes im Ereignisprotokoll registrieren: „Fehler 5722: Die Einrichtung einer Sitzung von Computer Computername ist an der Echtheitsbestätigung gescheitert. Der Kontenname in der Sicherheitsdatenbank ist Kontoname. Folgender Fehler ist aufgetreten: Text.“ Oder „Fehler 5723: Die Sitzung konnte von Computer Computername nicht eingerichtet werden, da kein Vertrauenskonto in der Sicherheitsdatenbank für diesen Computer vorhanden ist. Der Kontenname in der Sicherheitsdatenbank ist Kontoname.“

Dieses Authentifizierungsproblem scheint willkürlich aufzutreten und kann mehr als einen BDC betreffen. Das Problem lässt sich durch eine Installation von NT 4.0 Service Pack 4 (SP4) oder eine spätere Version lösen. Das Problem tritt auch bei NT Server 4.0, Terminal Server Edition (WTS) auf. Eine Installation von SP4 für WTS löst auch hier das Problem.

Begrenzen des Datenverkehrs Die PDCs zweier Domänen mit einer Trust-Beziehung können potenziell alle 15 Minuten Datenverkehr untereinander generieren. Das Intervall von 15 Minuten ist der Standardwert für den Registrierungsparameter ScavengeInterval. NT bestimmt mit Hilfe des Parameters ScavengeInterval, wann der Anmeldedienst verschiedene Arbeiten an einem PDC und BDCs verrichtet. Zu diesen Arbeiten gehören das Lokalisieren eines Domänen-Controllers, der Versuch, einen Namen „Domänenname [B1]NETBIOS“ einem BDC hinzuzufügen, das Erkennen, ob ein sicherer Kanal zu lange im Leerlauf war oder die Entscheidung, ob ein Kennwort für einen sicheren Kanal geändert werden muss. (NT-4.0- und NT-3.x-Domänen-Controller ändern Kennwörter alle sieben Tage automatisch, und der Anmeldedienst sucht standardmäßig alle 15 Minuten nach dieser Änderung.)

Der Parameter ScavengeInterval kann so eingestellt werden, um den Verkehrsfluss zu optimieren, da keine der vorangehenden Operationen von entscheidender Bedeutung ist. Zum Beispiel kann bei Verwendung einer geleasten Leitung, für die Gebühren nach dem vom Netzwerk generierten Netzwerkverkehrsvolumen berechnet werden, eine Optimierung des Parameters ScavengeInterval recht vorteilhaft sein. Darüber hinaus kann eine Feineinstellung des Parameters ScavengeInterval den Verkehr reduzieren, der durch das regelmäßige Polling von Domänen-Controllern durch Vertrauensbeziehungen über ein WAN generiert wird.

Wenn der Parameter ScavengeInterval auf einem PDC nicht vorhanden ist, muss mit Hilfe von regedt32 der entsprechende Subkey in der Registrierung geändert werden. Die folgenden Schritte sind dann zur Erstellung von ScavengeInterval und zur Anpassung der zugehörigen Standardeinstellung erforderlich:

1. Auswählen des Registrierungsschlüssels HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters.
2. Hinzufügen des Wertnamens ScavengeInterval.
3. Auswählen des Datentyps REG_DWORD.
4. Anpassen des dezimalen Datenwerts.

Der dezimale Standarddatenwert ist 900 Sekunden bzw. 15 Minuten. Der Datenwert umfasst einen Bereich von 60 bis zu 172.800 Sekunden (d.h. 1 Minute bis 48 Stunden). Der optimale Wert muss für die jeweilige Domäne ermittelt werden. (kl)

Domänenverwaltung von einer NT-Workstation

Die Verwaltung von Windows-NT-Domänen muss nicht unbedingt an einem Domänen-Controller stattfinden. Domänen können auch von einer NT-Workstation aus verwaltet werden. Dazu müssen die Client-basierten Verwaltungsprogramme von NT Server von der CD-ROM der NT-Server-4.0-Installation auf der Workstation installiert werden. Im Ordner \clients\srvtools\winnt\ muss die Datei setup.bat ausgeführt werden.

Die Dateien werden im Ordner \%systemroot%\system32 auf der NT-Maschine installiert. Diese Installation erstellt keine Verknüpfungen für den Benutzer, sondern kopiert lediglich die Dateien. Für die folgenden Tools müssen im Anschluss Verknüpfungen erstellt werden:

DHCP-Manager	**dhcpadmn.exe**
Systemrichtlinieneditor	**poledit.exe**
Remote Access Administrator	**rasadmin.exe**
Remoteboot Manager	**rplmgr.exe**
Server-Manager	**srvmgr.exe**
Services für Macintosh	**sfmreg.exe**
Benutzer-Manager für Domänen	**usrmgr.exe**
WINS-Manager	**winsadmn.exe**

Von der NT-Domäne zum Active Directory

Sicheres Upgrade

von Douglas Toombs

Ein Windows-NT-Netzwerk ist bei der Verwaltung der Netzwerkkonten, Gruppen und Anmeldedienste von seinen Domänencontrollern abhängig. Sie bilden sozusagen das Fundament, auf das alle anderen Server und verteilten Dienste im NT-Netz zugreifen. Kein Wunder, dass sich viele Administratoren davor scheuen, an diesen kritischen Stellen ein Upgrade auf Windows 2000 zu wagen. Doch wer die Migrationsschritte in der richtigen Reihenfolge durchführt, kann seine Domänencontroller ohne Schwierigkeiten auf Windows 2000 aufrüsten.

Domänencontroller können in zwei Kategorien unterteilt werden: primäre Domänencontroller (PDCs) und Sicherungs-Domänencontroller (BDCs). (Weitere Informationen über Domänencontroller enthält der Artikel von L. J. Locher auf Seite 28.) In einem NT-Netzwerk ist in der Regel eine von drei Konfigurationsarten für Domänencontroller anzutreffen. Die erste Konfiguration ist ein Einzeldomänenmodell (Single Domain Model), das aus nur einer Domäne besteht, die sowohl Benutzerkonten als auch Maschinenressourcen enthält. Das Einzeldomänenmodell ist das einfachste NT-Domänenmodell und lässt sich dementsprechend auch am einfachsten aufrüsten.

Die zweite Konfiguration ist das Hauptdomänenmodell (Master Domain Model), bei dem zwei oder mehrere Domänen über Vertrauensbeziehungen miteinander verbunden sind. Beim Hauptdomänenmodell werden alle Benutzerkonten und Gruppen für das Unternehmen in der Hauptdomäne (Master Domain) gespeichert, die manchmal auch als Kontendomäne (Accounts Domain) bezeichnet wird, während physische Ressourcen wie Dateien und Drucker in Ressourcendomänen eingerichtet werden. Die Ressourcendomänen stellen eine Einwegvertrauensbeziehung zur Kontendomäne her, sodass sie Benutzern vertrauen können, die in der Kontendomäne registriert sind. Diese Art der NT-Infrastruktur wird häufig in mittleren und großen Organisationen eingesetzt.

Die dritte Konfiguration ist das Modell mit mehreren Hauptdomänen (Multiple-Master Domain Model), das gewöhnlich in großen Unternehmen anzutreffen ist, deren Benutzer- und Gruppenkontenanforderungen bis an die Kapazitätsgrenzen von NT-Domänen heranreichen. Das Modell mit mehreren Hauptdomänen enthält eine oder mehrere Kontendomänen und häufig mehrere Ressourcendomänen. Jede Ressourcendomäne richtet eine Einwegvertrauensbeziehung zu jeder Kontendomäne ein. Benutzer, die in der Kontendomäne definiert sind, können daher auf die Ressourcen in der Ressourcendomäne zugreifen.

Eine weitere Konfigurationsart, das Modell mit vollständigen Vertrauensbeziehungen (Complete Trust Model), besteht aus Domänen, die untereinander beidseitige Vertrauensbeziehungen innerhalb einer Infrastruktur besitzen. Da Administratoren das Modell mit vollständigen Vertrauensbeziehungen jedoch nicht häufig implementieren, konzentrieren wir uns in diesem Artikel auf die Migration eines Hauptdomänenmodells, das aus einer Kontendomäne und einer Ressourcendomäne besteht. Die gleichen Prinzipien lassen sich analog auch auf die Migration von Modellen mit einer Einzeldomäne bzw. mehreren Hauptdomänen anwenden.

Vorsichtsmaßnahmen vor der Aktualisierung Bevor die Aktualisierung von Netzwerken in Angriff genommen wird und insbesondere bevor Domänencontroller migriert werden, sollte man sich auf jeden Fall vergewissern, dass eine funktionierende, lesbare Bandsicherung der Server zur Verfügung steht. Eine andere Vorsichtsmaßnahme, die ergriffen werden kann, besteht darin, einen neuen NT-Server im Netzwerk zu installieren, ihn als BDC zu definieren und ihm die Möglichkeit zu geben, sich vollständig mit dem PDC der Domäne zu synchronisieren, bevor die Domäne auf Windows 2000 aufgerüstet wird. Nach der kompletten Synchronisierung des BDC wird er aus dem Netzwerk genommen und gesichert, bis sicher feststeht, dass die Domänenmigration erfolgreich abgeschlossen wurde. Falls die Domäne wieder in ihren Zustand vor der Migration auf Windows 2000 zurückversetzt werden muss, nimmt man einfach den Windows-2000-Domänencontroller vom Netz. Dann wird der Ersatz-BDC wieder online geschaltet und vom BDC zum PDC heraufgestuft.

Migration von Kontendomänen Microsoft empfiehlt, zuerst den PDC für die Kontendomäne eines NT-Netzwerks umzustellen (d.h. die PDC-Maschine, in der Regel

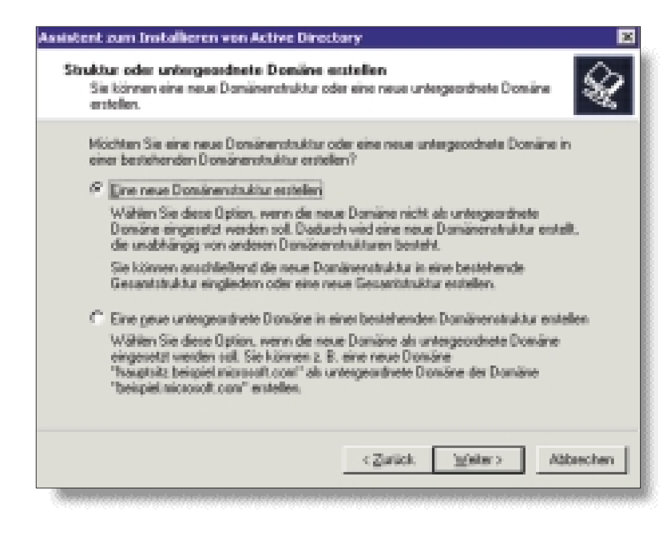


Bild 1. *Erstellen einer neuen Domänenbaumstruktur oder einer untergeordneten Domäne in einer bestehenden Domänenstruktur*

der erste Server, der installiert wurde, falls eine Einzeldomäne betrieben wird). Wenn gewährleistet ist, dass eine vollständige Systemsicherung erstellt wurde, kann die CD-ROM der Windows-2000-Installation in das CD-ROM-Laufwerk eingelegt werden, um die Aktualisierung zu beginnen. Ein Dialogfeld befragt den Benutzer, ob die vorhandene Installation von NT aktualisiert werden soll. Antwortet man mit „Ja“, wird der Setup-Assistent für Windows 2000 Server gestartet.

Bild 2. *Soll die Domäne eine eigene Gesamtstruktur darstellen oder in eine bestehende Gesamtstruktur integriert werden?*

Im Setup-Assistenten ist die Option zur Aktualisierung der vorhandenen Installation von NT auf Windows 2000 auszuwählen. Für den von uns aufgesetzten frisch installierten Test-PDC unter NT forderte der Setup-Assistent nur wenige Informationen zu Beginn des Aktualisierungsprozesses an und erkannte, dass es sich bei dem System um einen PDC handelte. Daher mussten keine domänenbezogenen Informationen eingegeben werden. Nachdem die angeforderten Informationen eingegeben waren, durchlief der Assistent den Aktualisierungsprozess. Der Benutzer sollte die Installationsroutine ungehindert ihre Arbeit erledigen und die Aktualisierung von NT auf Windows 2000 zu Ende führen lassen. Wenn die Aktualisierung abgeschlossen ist, führt Windows 2000 einen Neustart aus und meldet den Benutzer am Betriebssystem an, um den Rest des Migrationsprozesses in Angriff zu nehmen.

Nach dem automatischen Booten von Windows 2000 Server wird das Programm dcpromo.exe zur Heraufstufung von Domänencontrollern oder der Assistent zur Installation von Active Directory (Active Directory Installation Wizard) gestartet. Brechen Sie diesen Prozess bei der Aktualisierung eines PDC nicht ab. Dieses Programm ermöglicht dem Benutzer, Domänencontroller-Dienste auf einer Windows-2000-Maschine hinzuzufügen oder zu löschen, was unter NT 4.0 nicht ohne eine vollständige Neuinstallation des Betriebssystems möglich ist. DCPROMO erkennt die charakteristischen Merkmale der Domäne wie Name, Benutzer und Gruppen und stellt einige wenige Fragen. Anschließend beginnt der Prozess der Migration des Systems auf AD.

Zuerst überprüft DCPROMO die Kompatibilität des Computers mit Windows 2000 und stellt fest, ob das System über den Dienst zur Verzeichnisreplikation (Directory Replicator) verfügt. Falls Benutzer keine Anmeldeskripte im Netzwerk verwenden, sind sie sich der Existenz dieses Dienstes vielleicht gar nicht bewusst. Der Verzeichnisreplikationsdienst ist ein NT-Prozess, der Dateien (in den meisten Fällen Anmeldeskripte) zwischen Servern repliziert. NT-Server sind für die Replikation von Anmeldeskripten zwischen Systemen von diesem Dienst abhängig. Da jeder PDC oder BDC einen Benutzer im Netzwerk authentifizieren kann, muss der Benutzer eine Kopie des Anmeldeskripts auf jeder Maschine besitzen, die ihn authentifizieren kann. Windows 2000 unterstützt den Verzeichnisreplikationsdienst jedoch nicht, sodass eine alternative Lösung zur Behandlung der Anmeldeskripte benötigt wird (siehe Kasten „Replikation von Anmeldeskripten“).

Nun muss der Benutzer entscheiden, ob eine neue Domänenstruktur für das Unternehmen erstellt werden soll oder ob eine untergeordnete Domäne in einer vorhandenen Domänenstruktur eingefügt werden soll wie in Bild 1 zu sehen ist. Wenn die AD-Infrastruktur bei Erreichen dieser Anzeige im Voraus geplant wurde, sollte der Benutzer wissen, wie er zu reagieren hat. Für unser Beispiel nehmen wir an, dass eine neue Domänenstruktur erstellt werden soll, was sinnvoll ist, wenn die Migration aus einer Einzeldomäne heraus erfolgt. In diesem Fall ist die erste Option auszuwählen und anschließend auf „Weiter“ zu klicken.

Wie in Bild 2 zu sehen ist, fragt der Installationsassistent für Active Directory ab, ob aus dieser Domänenstruktur eine neue Gesamtstruktur erstellt werden soll oder ob sie in eine vorhandene Gesamtstruktur eingefügt werden soll. Wie bereits erwähnt, sollten bis zu diesem Zeitpunkt im Prozess bereits organisatorische Entscheidungen getroffen worden sein. Wenn keine andere Windows-2000-Installation innerhalb der Organisation vorhanden ist, kann angenommen werden, dass eine neue Gesamtstruktur für Domänen zu erstellen ist. Diese neue Domänenstruktur wird dann zur ersten Domänenstruktur in der Gesamtstruktur. In diesem Fall ist wiederum die erste Option auszuwählen und anschließend auf „Weiter“ zu klicken.

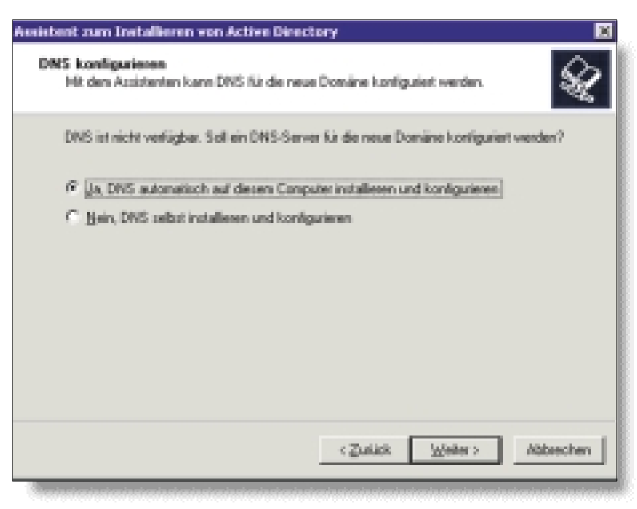


Bild 3. *Ohne Domain Name Server geht bei Active Directory gar nichts. Hier entscheiden Sie, ob Sie auf dem Domänencontroller auch DNS installieren wollen.*

Der Active-Directory-Installationsassistent führt den Benutzer anschließend durch verschiedene weitere Konfigurationsschritte für das System, zu denen

auch die DNS-Konfiguration gehört. Diese stellt einen wesentlichen Teil der Migration von Sicherungsdomänencontrollern (BDCs) dar. BDCs sind von der Verfügbarkeit einer Art von DNS-Dienst abhängig, um den früheren PDC ausfindig zu machen. Wenn ein Unternehmen keine DNS-Lösung implementiert hat, muss die Option zur Installation und Konfiguration von DNS auf dem PDC ausgewählt werden, der gerade aktualisiert wird (siehe Bild 3). In den verbleibenden Konfigurationsschritten muss der Benutzer Fragen zu den Dateipositionen zur Speicherung des AD und des gemeinsamen Systemdatenträgers (SYSVOL) beantworten. Nach der Beantwortung dieser Fragen erreicht der Benutzer den letzten Schritt von DCPROMO, in dem er die Standardberechtigungen für Benutzer- und Gruppenobjekte auswählt, wie in Bild 4 zu erkennen ist.

In diesem letzten Schritt fordert der Installationsassistent den Benutzer auf, Berechtigungen nach ihrer Kompatibilität mit Servern unter NT-Versionen vor Windows 2000 oder reinen Windows-2000-Servern festzulegen. Einige Anwendungen und Dienste in NT-Netzwerk arbeiten mit anonymen oder NULL-Sitzungen, um Domänencontroller nach Benutzerinformationen abzufragen. Zum Beispiel verwendet RAS auf einem NT-Mitglieds-Server in der Regel eine NULL-Sitzung zur Abfrage eines Domänencontrollers, um festzustellen, ob Benutzer sich in das Netzwerk einwählen können oder ob der Server die Benutzer zurückrufen muss. Diese Möglichkeit von NULL-Sitzungen kann auf Windows-2000-Domänencontrollern zur Erhöhung der Sicherheit deaktiviert werden. Bevor jedoch diese Möglichkeit ausgeschaltet wird, ist sicherzustellen, dass keine der Server-Anwendungen eine NULL-Sitzung zur Abfrage eines Domänencontrollers nach Benutzerinformationen benötigt. Man könnte die RAS-Server unter NT zuerst auf Windows 2000 aktualisieren. Falls RAS auf einem BDC ausgeführt wird, spielen NULL-Sitzungen keine Rolle. In diesem Fall besitzt der Server eine lokale Kopie der Konteninformationen, sodass er keine NULL-Sitzung zur Abfrage eines Domänencontrollers nach diesen Informationen benötigt.

Wenn die Fragen des Installationsassistenten beantwortet sind, beginnt Windows 2000 mit der Installation des AD und mit der Umwandlung der vorhandenen Daten in das AD-Format. Nach Abschluss dieses Prozesses verfügt der Benutzer über einen funktionsfähigen AD-Domänencontroller auf der Maschine, die zuvor der PDC unter NT 4.0 war.

Zwei Gesichter Obwohl Active Directory jetzt auf dem früheren PDC installiert wurde, können die anderen, noch nicht aktualisierten Domänencontroller die Änderungen, die am PDC vorgenommen wurden, nicht erkennen. Neu installierte Windows-2000-Domänencontroller arbeiten in einem gemischten Modus, was bedeutet, dass sie als AD-Domänencontroller fungieren und gleichzeitig PDCs früherer Versionen emulieren können. Die neuen Windows-2000-Domänencontroller werden also den alten PDC emulieren, und die anderen BDCs im Netzwerk werden diese Änderungen nicht bemerken. Allerdings können einige der wichtigeren Windows-2000- und AD-Funktionen erst aktiviert werden, wenn die Systeme vom gemischten Modus in den AD-spezifischen Modus umgeschaltet werden. Zum

Beispiel könnte es sinnvoll sein, die Multimaster-Replikation zu aktivieren, bei der beliebige Domänencontroller Änderungen an AD-Informationen vornehmen und anschließend diese Änderungen auf die anderen Domänencontroller im Netzwerk übertragen können.

Der Wechsel zum AD-spezischen Modus kann erst durchgeführt werden, wenn alle Domänencontroller im gesamten Netzwerk in einen AD-fähigen Status versetzt wurden. Dieser Wechsel zum spezifischen AD-Modus kann jedoch nicht mehr rückgängig gemacht werden, da diese Operation nur in eine Richtung funktioniert.

BDC-Migration Den nächsten Schritt des Aktualisierungsprozesses bildet die Migration der BDCs. BDCs werden auf ähnliche Weise aktualisiert wie PDCs. Vor der Aktualisierung der BDCs muss jedoch sicher gestellt werden, dass DNS-Dienste im Netzwerk funktionieren und dass die BDCs diese Dienste erreichen können. Wenn DNS-Dienste im Rahmen der PDC-Aktualisierung hinzugefügt wurden, kann mit dem BDC-Aktualisierungsprozess fortgefahren werden. Wurden die DNS-Dienste dem PDC nicht hinzugefügt bzw. ein anderer DNS-Server während der Aktualisierung verwendet, müssen Sie die IP-Adressinformationen vor der Aktualisierung der BDCs zur Hand haben.

Wenn das Programm DCPROMO gestartet wird, erkennt es, dass die Maschine zuvor als BDC eingesetzt war und stellt einige Fragen, die sich leicht von den Fragen bei der PDC-Aktualisierung unterscheiden. Zum Beispiel bietet DCPROMO nun die Option an, entweder den BDC in seiner Funktion als Domänencontroller zu belassen oder die Domänencontroller-Dienste vom BDC völlig zu entfernen. Sofern keine strukturellen Änderungen während des Aktualisierungsprozesses am Netzwerk vorgenommen werden, sollte dieser Server als Domänencontroller beibehalten werden. Die entsprechenden Dienste lassen sich auch später noch entfernen, wenn sie nicht benötigt werden.

DCPROMO führt den Benutzer durch die Einrichtung dieses BDC als weiteren Domänencontroller in der Domänenstruktur, die zuvor definiert wurde. Das Programm fordert die Eingabe eines Benutzernamens, eines Kennworts und einer Domäne an, die für die Windows-2000-Domäne verwendet werden, der der Domänencontroller hinzugefügt wird. Wie bei einer NT-4.0-Installation bildet dieser Schritt eine Sicherheitsprüfung für den ersten Synchronisierungsprozess. Der Benutzer muss ein administratives Konto mit entsprechendem Kennwort in die AD-Domäne eingeben und auf „Weiter“ klicken.

Die restlichen, von DCPROMO gestellten Fragen stimmen mit den denjenigen überein, die bereits bei der Migration des PDC gestellt wurden (z.B., wo die AD-Dateien und die SYSVOL-Dateien gespeichert werden sollen). Geben Sie für jeden Schritt im Prozess die angeforderten Informationen ein und klicken Sie auf „Weiter“. Nach der Eingabe aller Informationen, die DCPROMO zur Einrichtung dieses Domänencontrollers benötigt, beginnt es mit dem Installationsprozess, um den BDC in einen Domänencontroller in der AD-Domäne umzuwandeln.

Migration von Ressourcendomänen Nach der Migration der gesamten Kontendomäne nach AD werden die Ressourcendomänen aktualisiert, sofern

Replikation von Anmeldeskripten

Da Windows 2000 den Verzeichnisreplikationsdienst nicht mehr unterstützt, muss eine alternative Methode zur Replikation von Anmeldeskripten unter Windows-2000-Domänencontrollern entwickelt werden. Microsoft verwendet den automatisierten Dateireplikationsdienst, eine Schlüsselkomponente des verteilten Dateisystems DFS, um Dateiverzeichnisse Server-übergreifend in einem Windows-2000-Netzwerk zu synchronisieren.

Während der Windows-2000-Installation wird der Dateireplikationsdienst automatisch so konfiguriert, dass das Verzeichnis des gemeinsamen Systemdatenträgers SYSVOL (standardmäßig in \%systemroot%\sysvol gespeichert) auf alle Domänencontrollern im Netzwerk repliziert wird. Die Anmeldeskripte können deshalb in die SYSVOL-Verzeichnisstruktur verlegt werden, um sie im gesamten Windows-2000-Netzwerk zu replizieren.

Falls jedoch der PDC als Export-Server für die Anmeldeskripte konfiguriert ist und die BDCs als Import-Server fungieren (eine recht gängige Konfiguration), kann es zu einem Problem kommen, wenn der PDC zuerst migriert wird. Die Replikation von Anmeldeskripten in der gesamten Konfiguration wird effektiv ausgeschaltet, wenn der Export-Server zuerst aktualisiert wird. Aus diesem Grund empfiehlt Microsoft, einen anderen Server als Export-Server im Netzwerk zu definieren und dieses System erst nach der Migration aller anderen Systeme auf Windows 2000 zu aktualisieren.

solche vorhanden sind. Wenn die Ressourcendomänen in derselben Domänenstruktur aktualisiert werden sollen wie die Kontendomäne, ist es wahrscheinlich sinnvoll, zunächst die lokalen Administratoren aus den administrativen Gruppen der Ressourcendomäne zu entfernen. Dieser Schritt ist nötig, weil durch die Aktualisierung auf Windows 2000 eine beidseitige Vertrauensbeziehung zwischen der untergeordneten (Ressourcen-) und der übergeordneten (Konten-)Domäne hergestellt wird. Wenn unter NT ein Hauptdomänenmodell implementiert war, besaßen die unter- und übergeordneten Domänen lediglich eine Vertrauensbeziehung in einer Richtung, nämlich von der untergeordneten zur übergeordneten Domäne. Bei der Herstellung einer beidseitigen Vertrauensbeziehung erhalten Benutzer, die nur über Administratorberechtigungen für die Ressourcendomäne verfügten, auch Administratorberechtigungen für die Kontendomäne. Wenn Sicherheit eine wichtige Rolle spielt, ist es ratsam, die Administratorberechtigungen von Benutzern in der Ressourcendomäne aufzuheben, denen in der Hauptdomäne (Kontendomäne) keine administrativen Zugriffsrechte erteilt werden sollen.

Wenn alles zur Migration der Ressourcendomänen vorbereitet ist, können die Ressourcendomänen in derselben Abfolge von Schritten wie die Kontendomäne umgestellt werden: jeweils die PDCs zuerst und anschließend die BDCs. Die gesamte Infrastruktur kann so von einer Domäne zur nächsten abgearbeitet werden, um alle Domänencontroller auf Windows 2000 Server zu migrieren.

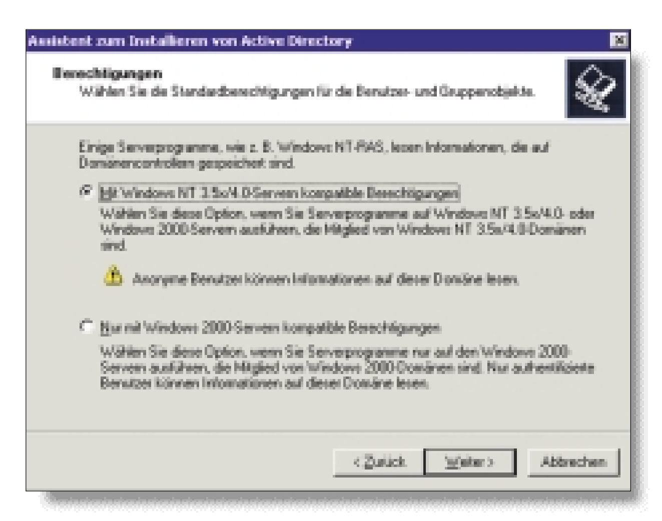


Bild 4. *Auswählen der Standardberechtigungen für die Benutzer- und Gruppenobjekte*

Wechseln zum AD-spezifischen Modus Wenn die Migration sämtlicher NT-Domänencontroller abgeschlossen ist, kann vom Betrieb des gemischten Modus zum AD-spezifischen Betriebsmodus gewechselt werden. Windows 2000 Professional ist standardmäßig für Active Directory eingerichtet. Auf anderen Betriebssystemen muss zuerst die Active-Directory-Client-Software installiert werden, damit sie den Verzeichnisdienst erkennen können. (AD-Clients sind zur Zeit nur für Windows 9x verfügbar.)

Starten Sie die Verwaltung von Active-Directory-Domänen und Vertrauensstellungen und wählen Sie die Domäne aus. Durch Klicken mit der rechten Maustaste auf die Domäne und Auswählen der Option Eigenschaften kommen Sie zu dem Dialog, der in Bild 5 zu sehen ist.

Im unteren Teil der Eigenschaftenseite wird signalisiert, dass die Domäne im gemischten Modus arbeitet. Um die Domäne in den einheitlichen Modus zu konvertieren, müssen Sie auf „Modus wechseln“ klicken. Wie bereits erläutert, handelt es sich hierbei um eine einmalige Operation, die nur in eine Richtung funktioniert, sodass sichergestellt werden muss, dass die Änderung des Modus ordnungsgemäß vorbereitet ist, bevor die Operation

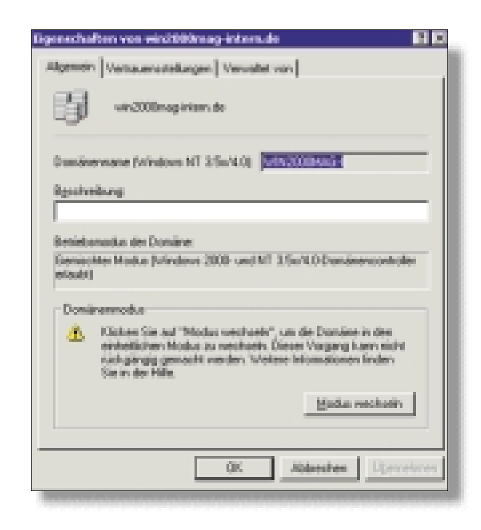


Bild 5. *Ändern der Domäne vom gemischten Modus in den einheitlichen Modus*

fortgesetzt wird. Eine Anzahl von Dialogfeldern weist den Benutzer darauf hin, dass der Moduswechsel nicht rückgängig zu machen ist. Wenn die Domäne jedoch vorbereitet entsprechend vorbereitet wurde, kann die Änderung durchgeführt werden. Der Wechsel zum AD-spezifischen Modus kann einige Minuten dauern, während deren die Domänencontroller untereinander kommunizieren. Wenn der Wechsel abgeschlossen ist, stehen sämtliche AD-Funktionsmerkmale zur Verfügung. (fbi)

Hotline

In dieser Ausgabe des Windows 2000 Magazins haben wir Hotline-Fragen und -Antworten zu Windows NT 4.0 zusammengestellt. Natürlich werden Sie hier in künftigen Ausgaben auch Problemlösungen für Windows 2000 finden.

- verlorener CD-Key
- Blessuren beim Systemstart
- Dr. Watson ausschalten
- Notfalldiskette erstellen
- Installationsfehler bei IIS
- eigene Logon-Meldung
- Prioritäten für Anwendungen
- Recovery für Software-RAID
- Regclean
- Tools für Registry-Anpassung
- Globale Umgebungsvariablen
- Vorsicht bei Rollback.exe
- Zugriff auf Systemsteuerung
- Letzter angemeldeter Benutzer
- „Leichen" in der Software-Liste
- Shortcut für Systemsteuerungs-Applets

? Kann man den CD-Key bei Verlust der NT-Lizenz aus der Registry wieder auslesen?

Starten Sie das Programm regedit.exe und begeben Sie sich zu folgendem Schlüssel:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows NT\Current
Version
```

Hier finden Sie unter ProductId einen Zahlenwert, von dem die Ziffern 6 bis 15 Ihrem CD-Key entsprechen.

Hinweis: Der CD-Key kann ebenfalls mit dem NT-Diagnose-Tool ausgelesen werden. Auch hier sind es die Ziffern 6-15.

? Welche Ursache könnte ein Blue-Screen-Absturz beim Startvorgang mit der Fehlermeldung: `IRQL_NOT_LESS_OR_EQUAL` haben?

Das bedeutet meist, dass ein Gerätetreiber versuchte, auf einen Speicherbereich zuzugreifen, auf den er nicht zugreifen darf. Welche Adressen im Spiel sind und welcher Treiber der Schuldige ist, kann normalerweise der Meldung entnommen werden. Diese hat meist folgenden Aufbau:

```
STOP 0x0000000A
(0xWWWWWWWW, 0xXXXXXXXX,
0xYYYYYYYY,0xZZZZZZZZ)
IRQL_NOT_LESS_OR_EQUAL ** Address
0xZZZZZZZZ has base at <address>-
<driver>
```

Dabei bedeutet:

- 0xWWW: Die Adresse, die falsch angesprochen wurde
- 0xXXX: Der IRQL, der für den Zugriff benötigt wurde
- 0xYYY: Art des Zugriffs (0=lesen, 1=schreiben)
- 0xZZZ: Adresse der Instruktion, die versuchte, den Zugriff durchzuführen.

In der Zeile **Adresse... wird der „schuldige" Treiber angegeben.

? Kann man Dr. Watson ausschalten, der ja bei Programmfehlern automatisch vom System gestartet wird?

Dies ist möglich durch eine Änderung in der Registry. Starten Sie das Programm regedit.exe und begeben Sie sich zu folgendem Schlüssel:

```
HKEY_LOCAL_MACHINE\Software\
Microsoft\Windows NT\Current
Version\AeDebug
```

Löschen Sie einfach den Schlüssel, wenn Dr. Watson nicht mehr ausgeführt werden soll.

Um Dr. Watson wieder zu starten, geben Sie

```
drwtsn32 -i ein.
```

? Wie erstellt oder aktualisiert man eine Notfalldiskette?

Sie haben die Möglichkeit, mit dem Befehl rdisk eine Notfalldiskette zu erstellen oder eine bestehende zu aktualisieren. Hierfür gibt es zwei Optionen, die mit diesem Befehl verwendet werden können:

rdisk /s Speichern einschließlich Default, Sam and Security Dateien und Dialog zur Erstellung einer Notfalldiskette.

rdisk /s- Speichern einschließlich Default, Sam and Security Dateien ohne Erstellung einer Notfalldiskette.

? Wie vermeidet man die Installationsfehler des Internet Information Server (IIS)?

Die Installation des Internet Information Server von der Windows NT 4.0 Server CD ist nicht fehlerfrei. Bei der Installation werden zwei Dateien überspielt. Um diesen Fehler zu umgehen, müssen Sie die Dateien ODBCINT.DLL und ODBCCP32.DLL vor der Installation an einen „sicheren Ort" kopieren und nach erfolgter Installation wieder in das Verzeichnis winnt\system32\ zurückkopieren.

? Kann ich meine eigene Logon-Meldung definieren?

Um die Standardmeldung zu ändern, gehen Sie folgendermaßen vor: Starten Sie das Programm regedit.exe und begeben Sie sich zu folgendem Schlüssel:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows NT\Current
Version\Winlogon
```

Unter LogonPrompt – >Reg_SZ. können Sie bei Wert jede beliebige Zeichenfolge, jedoch auf max. 255 Zeichen begrenzt, eingeben.

? Kann man eine Real-Time-Anwendung mit hoher Priorität starten?

Geben Sie einen Befehl mit folgenden Parametern in der DOS-Eingabeaufforderung ein:

```
start /<Priorität> <Applikation>
```

Sie möchten beispielsweise das Programm Explorer mit hoher Priorität starten. Geben Sie wie oben angeführt folgenden Befehl ein:

```
start /high explorer.exe
```

Hinweis: Eine komplette Liste der möglichen Optionen erhalten Sie, wenn Sie start /? eingeben.

? Ich habe ein Software-RAID auf meinem Computer installiert. Wie kann ich sichergehen, dass ich nach einer Neuinstallation meine Daten wiederherstellen kann?

Starten Sie dafür den Festplattenmanager und wählen Sie im Menü Partition Konfiguration-Speichern... Nach einer Neuinstallation können Sie unter Konfiguration-Wiederherstellen Ihre Daten, die sich beispielsweise in einem Stripe Set befunden haben, regenerieren.

? Kann man die Komponenten der Systemsteuerung direkt aus dem Explorer oder mittels Shortcut aufrufen?

Ja. Es gibt für jede Komponente der Systemsteuerung eine .CPL-Datei im Systemverzeichnis von NT. Hier eine Auflistung der CPL-Dateien:

Datei	Beschreibung
ACCESS	Eingabehilfe
APPWIZ	Software hinzufügen/entfernen
CONSOLE	Konfiguration der DOS-Box
DESK	Anzeige
DEVAPPS	PCMCIA-Controller
INETCPL	Konfiguration der Internet-Einstellungen
INTL	Ländereinstellungen
MAIN	Konfiguration der Maus
MMSYS	Multimedia
MODEM	Konfiguration der Modems
NCPA	Konfiguration der Netzwerkeinstellungen
PORTS	Konfiguration der Anschlüsse/Schnittstellen
SYSDM	Systemeigenschaften
TELEPHON	Wahlparameter
TIMEDATE	Einstellungen für Datum/Uhrzeit

Die Anzahl der CPL-Dateien kann ja nach installierter Hard- und Software unterschiedlich sein. Die Auflistung beschränkt sich auf die wichtigsten mit dem Betriebssystem installierten Komponenten.

? Welche Möglichkeiten bietet das von Microsoft im Internet zum Download angebotene Programm „Regclean“ an?

Mit diesem Programm ist es möglich, die Registry nach ungültigen, bzw. fehlerhaften Einträgen zu durchsuchen und die betreffenden Einträge auch direkt zu bereinigen. Benutzen Sie immer die aktuellste Version, da es sonst zu Problemen kommen kann.

? Welche Tools gibt es für Registry-Anpassungen?

Für alle, die Registry-Änderungen per Tool durchführen möchten, hat Microsoft die „Power Toys“ entwickelt. Besonders interessant ist das Freeware-Programm Tweak UI. Mit diesem Werkzeug können Sie Einstellungen an Ihrem Desktop vornehmen. Sie können sich die Power Toys kostenlos (Freeware) von der Microsoft-Seite aus dem Internet heruntergeladen.

Achtung:

Die Power Toys sind eigentlich für Windows 95 entwickelt worden. Später wurden die Anpassungen für NT implementiert, es sind jedoch immer noch nicht alle Programme unter NT lauffähig.

? Ich möchte Umgebungsvariablen in Batch-Dateien einsetzen. Dabei stellte ich fest, dass dies mit den Standard-Tools von NT nicht möglich ist. Welche Alternativen gibt es?

Abhilfe schafft das Programm setx.exe, das im Resource-Kit enthalten ist. Sie können damit Variablen setzen, die für das komplette System Gültigkeit haben.

Studieren Sie vor Einsatz des Programms ausgiebig die Hilfe, da die Syntax einen erfahrenen Anwender erfordert.

? Welche Vorsichtsmaßnamen muß man bei der Anwendung des Programms „rollback.exe“ treffen?

Achtung! Beim Ausführen überschreibt dieses Programm sofort ohne Sicherheitsabfrage die komplette Registry. Es gibt danach keine Möglichkeit mehr, das System wiederherzustellen!

Das Programm „rollback.exe“ wird standardmäßig nicht installiert.

Es befindet sich auf der Windows-NT-CD im Verzeichnis/support/deptools/i386.

? Wie kann man den Zugriff auf die Systemsteuerung durch Andere verhindern?

Sie brauchen nur die Zugriffsrechte auf die Dateien mit der Endung cpl sperren, die sich im Verzeichnis C:\Winnt\System32 befinden.

Da auch die Systemdialoge wie die Eigenschaften des Bildschirms in CPL-Dateien hinterlegt sind, kann der Anwender z.B. auch keine Änderungen mehr am Bildschirmschoner oder dem Hintergrundbild vornehmen.

? Kann man im Anmeldefenster von Windows NT durch einen Registry-Eintrag verhindern, dass der letzte Anwender angezeigt wird?

Starten Sie das Programm regedit.exe und wechseln Sie zu folgendem Eintrag:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows NT\Current
Version\Winlogon
```

Bei dem Eintrag: DontDisplayLastUserName bedeutet der Wert „0“, dass der Login-Name angezeigt wird und der Wert „1“, dass der Login-Name nicht angezeigt wird.

? Des öfteren stellte ich nach dem Entfernen von Software fest, dass der Eintrag nicht aus der Liste gelöscht worden ist? Was kann man dagegen unternehmen?

Durch Bearbeiten in der Registry können Sie diese Einträge löschen.

Starten Sie das Programm regedit.exe und begeben Sie sich zu folgendem Schlüssel:

```
HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\CurrentVersion\
Uninstall
```

Hier sind alle Programme aufgeführt. Programme, die nicht beim Entfernen ausgetragen wurden, können Sie hier manuell löschen. (kl)

Unsere Hotline-Partner

DVMB
E-Mail: Support@dvmb.de

Tricks & Traps

Lassen Sie andere NT- und Windows-2000-Anwender an Ihrem Erfahrungsschatz teilhaben. Schicken Sie Ihre Tipps an Redaktion@win2000mag.de.

In dieser Ausgabe:

- Remote-Zugriff auf Exchange Server
- DSL und Proxy-Server
- Datenträgernutzungsanalyse
- Datei-Cache-Manipulation
- Über Netware angeschlossene Drucker

1 Einige unserer Remote-Laptop-Benutzer wählen sich zum RAS-Server unserer Firma ein, um Microsoft Outlook 98 zu starten. Der Outlook-Client gibt eine Meldung aus, dass die Netzwerkverbindung nicht verfügbar ist. Die Laptop-Benutzer können alle Rechner im Netzwerk mit dem Ping-Befehl ansprechen und sie in der „Netzwerkumgebung" anzeigen, aber sie können keine Verbindung zu Microsoft Exchange Server herstellen. Einige Benutzer überwinden dieses Problem, indem sie ständig auf „Wiederholen" klicken, aber diese Methode ist sehr lästig. Sollten wir mit einem WINS-Server arbeiten?

Ein WINS-Server kann das Problem vielleicht lösen, insbesondere, wenn der Exchange Server mindestens einen Router-Sprung vom RAS-Server entfernt ist (weil ein Host in einem Netzwerk ohne Namens-Server keine Broadcasts zur Auflösung des Namens eines anderen Host-Systems verwenden kann). Darüber hinaus sollte die WINS-Server-Adresse in die Adressfelder sowohl für den primären als auch für den sekundären WINS-Server im Dialogfeld zur Konfiguration der TCP/IP-Eigenschaften auf dem RAS-Server eingetragen werden. Dieses Verfahren hilft sicherzustellen, dass die RAS-Clients die richtigen WINS-Server-Adressen vom RAS-Server erhalten.

Für andere potenzielle Lösungen ist jedoch kein WINS erforderlich. Zum Beispiel kann auf den RAS-Clients ein Eintrag für den Exchange-Server in die Datei LMHOSTS oder HOSTS eingefügt werden. (Zur Erzielung der besten Leistung ist es empfehlenswert, die Datei HOSTS zu verwenden.) Allerdings ist diese Lösung schwieriger zu implementieren und zu verwalten als die WINS-Lösung und verursacht mehr administrativen Aufwand. Alternativ kann auch dafür gesorgt werden, dass Service Pack 4 (SP4) oder eine höhere Version auf allen betroffenen Windows-NT-Maschinen (d.h. RAS-Clients, RAS-Servern und Exchange-Servern) installiert wird. Auf NT-Maschinen vor SP4 kommt es augenscheinlich zu mehr Problemen mit der Namensauflösung als auf Maschinen mit SP4 oder einer späteren Version. Wenn in der Vergangenheit Einträge in der Datei LMHOSTS zur Lösung von Problemen mit der Namensauflösung für RAS-Clients verwendet wurden, können die Probleme nach der Installation von SP4 wieder auftreten. Wenn dies der Fall ist, kann die Datei LMHOSTS auf dem Client umbenannt oder gelöscht werden. Anschließend muss mit dem NetBT-Statistikdienstprogramm Nbtstat (NetBT – NetBIOS over TCP/IP) der NetBIOS-Namens-Cache wieder geladen werden. Geben Sie dazu Folgendes in eine Befehlszeile ein:

```
nbtstat -rr
```

Alternativ dazu können Sie das System auch einfach erneut starten.

Eine andere potenzielle Ursache des Problems steht nicht im Zusammenhang mit der Namensauflösung. Die Meldung, dass die Netzwerkverbindung nicht verfügbar ist, könnte auch angezeigt werden, wenn Benutzer das Netzwerk des Exchange-Servers von einer lokal authentifizierten NT-Workstation (im Gegensatz zu einer Workstation, die in der Domäne des Exchange-Servers authentifiziert wird) aus anwählen. In diesem Fall kann das Problem entschärft werden, indem Sie auf das Outlook-Profil zugreifen und die Konfiguration des Exchange-Server-Dienstes ändern. Im Dialogfeld für Eigenschaften des Exchange-Server-Dienstes wählen Sie die Registerkarte für erweiterte Optionen aus und ändern den Wert für Anmeldenetzwerk in Kein. Dieses Verfahren zwingt den Client, sich explizit von der Domäne des Exchange-Servers authentifizieren zu lassen, bevor er versucht, die Verbindung mit Hilfe der Anmeldeinformationen des lokal angemeldeten Benutzers herzustellen.

2 Ich habe meine alte Wählverbindung zum Internet und den Internet-Dienstanbieter (ISP) durch eine neue Digital Subscriber Line (DSL) und einen ISP-Dienst ersetzt. In dem alten Szenario konnte ich mit Microsoft Proxy Server 2.0 auf das Internet von meiner Workstation aus zugreifen. Mit der neuen DSL-Konfiguration kann ich jedoch nicht mit dem Proxy-Server von meiner Workstation aus auf das Internet zugreifen. DSL verwendet eine Netzwerkkarte (NIC) und eine DSL-Bridge bzw. einen Router. (Ich verwende eine Bridge.) Ich habe keinen freien PCI-Platz, sodass dem Server keine weitere NIC hinzugefügt werden kann, und ich möchte keine ISA-Karte verwenden. Wie kann ich einen Proxy-Server oder Router einsetzen, um von der Workstation aus auf das Internet zuzugreifen?

Sie können die DSL-Verbindung für den Server und die internen Workstations nutzen. Beginnen Sie damit, dass Sie die Option zum automatischen Wählen des Proxy-Servers deaktivieren, die von der vorigen Konfiguration zum Wählen auf Anforderung wahrscheinlich aktiviert wurde. DSL ist eine permanent aktive Technologie, sodass RAS nicht zum Wählen der Verbindung verwendet werden muss. Als Nächstes müssen Sie eine zweite IP-Adresse (Schnittstelle) auf dem Windows-NT-Server für die zu verwendende DSL-Verbindung (das Netzwerksegment, das mit der DSL-Bridge verbunden wird) konfigurieren. Obwohl die beste und sicherste Methode zur Herstellung dieser Konfiguration in der Verwendung einer zweiten NIC besteht, der die vom ISP erteilte IP-Adresse zugewiesen wird, nehme ich für diese Erläuterung an, dass Sie nur eine NIC verwenden.

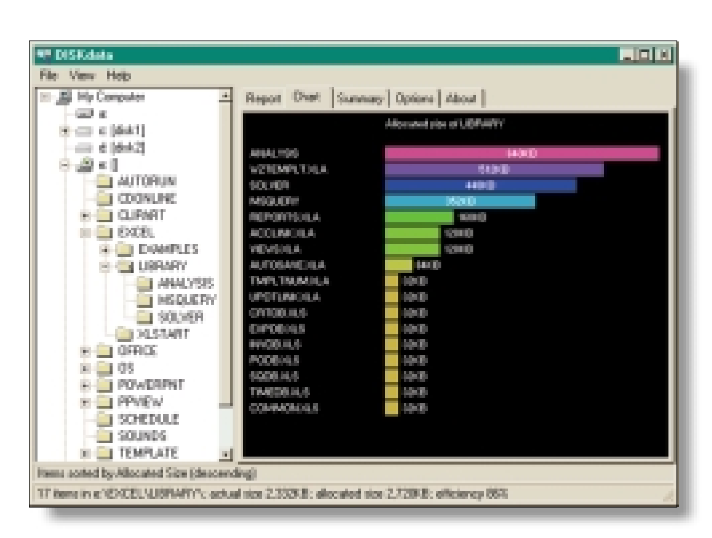
Weisen Sie der NIC auf dem Server eine zweite IP-Adresse zu. Dann stellen Sie sicher, dass die DSL-Bridge mit dem gleichen Hub wie der Server und die Workstation verbunden ist. In dieser Konfiguration werden im Prinzip zwei getrennte logische IP-Subnets über ein Ethernet-Segment betrieben. (Sie könnten z.B. eine private oder nicht Routing-fähige Adresse 10.1.1.1 für die Verbindung zum privaten, internen Netzwerk und eine Routing-fähige IP-Adresse 204.56.55.202 für die Verbindung zu der DSL-Bridge haben.) Nach der Überprüfung auf korrekte Proxy-Server-Konfiguration und einem Neustart des Servers können Sie auf die DSL-Internet-Verbindung von der Workstation aus über den Proxy-Server zugreifen.

Diese Prozedur habe ich erst vor kurzem für einen meiner Microsoft Small-

Business-Server-(SBS-)Clients durchgeführt, der gerade von einer Wählverbindung auf DSL umgestellt worden war. Allerdings entdeckte ich einen Fehler, bei dem der Proxy-Server ständig seine eigene Web-Seite anstelle der beabsichtigten Web-Site den Proxy-Clients anbot, die versuchten, über einen Browser auf das Internet zuzugreifen. Die Lösung dieses Problems bestand in der Installation von Service Pack 4 (SP4 – ein neueres Service Pack hätte auch funktioniert) auf dem Server.

Probleme beim gemischten Einsatz von ISA und PCI habe ich nicht festgestellt. Allerdings bevorzuge ich PCI-Karten, weil sie leichter zu verwalten sind und tendenziell weniger Belastung für die System-CPU generieren. Wenn Sie keinen PCI-Einbauplatz frei machen können, können Sie die aktuelle NIC durch eine PCI-NIC mit zwei Ports (dual port), zum Beispiel von Intel oder Adaptec, ersetzen.

3 Ich benötige eine kleine, schnelle und effiziente Anwendung, die die Größe der Basisverzeichnisse von Benutzern berechnet. In unserem Netzwerk enthalten diese Ordner eine große Menge von Daten, und ich möchte den Platzbedarf analysieren und die Verzeichnisse (und Unterverzeichnisse) der Größe nach sortieren. Der begrenzte Funktionssatz des Dienstprogramms Diruse aus dem Microsoft Windows NT Server 4.0 Resource Kit konnte dieses Problem nicht lösen. Gibt es andere Möglichkeiten?



Analyse der Speicherausnutzung mit Diskdata

Zur Durchführung einer Plattennutzungsanalyse sollten Sie das Dienstprogramm „Diskdata“ von Digital Information Gallery (http://www.digallery.com/Diskdata) testen. Auf dem Bild ist Diskdata in Aktion zu sehen. Dieses handliche Dienstprogramm bietet eine Windows-Explorer-ähnliche grafische Benutzerschnittstelle (GUI) und analysiert die Plattenspeichernutzung über verschiedene Volumes und Ordner hinweg. Diskdata kann die Nutzung in Berichts- oder Diagrammform anzeigen. Zu den verfügbaren Statistikergebnissen in Report- oder Diagrammformat gehören Datei- und Ordnergröße, zugeordnete Größe, Speicherbelegung, Änderungsdatum, Attribute und Versionsinformationen.

4 Windows NT 4.0 bietet ein umfangreiches Speichermanagement, neigt jedoch dazu, eine beträchtliche Datei-Cache-Größe zu verwenden. Mein System verfügt über 64 MB Arbeitsspeicher, und ich möchte den physischen Speicher effektiver für Anwendungen nutzen. Der Task-Manager meldet, dass der physische Speicher nur 30 MB beansprucht, während der Datei-Cache ca. 10 bis 18 MB verwendet. Wie lässt sich die Datei-Cache-Größe auf dem System verringern?

Virtual Memory Manager (VMM) von NT ordnet den Speicher dynamisch zwischen dem System-Cache (den NT als Netzwerk- und Datei-Cache nutzt) und dem Speicher zu, der für Systemprozesse einschließlich Anwendungen zur Verfügung steht. Diese Zuordnung erfolgt ohne Unterbrechung, abhängig davon, welche Auslastung das System in der Speichernutzung erfährt. Allerdings beeinflussen die folgenden Faktoren die Formeln, nach denen NT diese Zuordnungen vornimmt:

◆ Die Verwendung von NT Server oder NT Workstation.

◆ Die Konfiguration des Server-Dienstes, die Registrierungswerte ändert, die sich wiederum auf die System-Cache-Größe auswirken.

◆ Die Konfiguration anderer Dienste und Registrierungswerte, die sich auf die System-Cache-Größe auswirken.

NT Server ermöglicht eine Feineinstellung der Speicherzuordnung zwischen Prozessen und dem System-Cache. Das in Bild 2 gezeigte Dialogfeld wird über die Registerkarte „Dienste“ im Applet „Netzwerk“ der Systemsteuerung aufgerufen. Aktivieren Sie den „Server-Dienst“ und anschließend die „Eigenschaften“. Folgende Auswahlmöglichkeiten werden angeboten:

◆ Genutzten Speicher minimieren – minimiert die Speichernutzung für den Datei-Cache.

◆ Balance – Sorgt für gleichmäßige Speicherverteilung zwischen dem Cache und den aktiven Prozessen.

◆ Durchsatz für Dateifreigaben maximieren – Begünstigt die Speichernutzung für den Datei-Cache des Systems.

◆ Durchsatz für Netzwerkanwendungen maximieren – Begünstigt die Speichernutzung für Anwendungen.

Diese Einstellungen steuern, wie NT Speicher zwischen dem System-Cache und den Server-Diensten zuordnet und beeinflussen deshalb die Größe des System-Cache. Die Standardeinstellung für NT Server ist die Option zum Maximieren des Durchsatzes für Dateifreigaben, durch die der Registrierungs-Key LargeSystemCache im Subkey HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management auf 1 gesetzt wird.

NT Workstation stellt die Option der Eigenschaften für den Server-Dienst nicht zur Verfügung. Allerdings arbeitet NT Workstation standardmäßig mit der Option zum Minimieren des genutzten Speichers, wodurch LargeSystemCache auf den Wert 0 gesetzt wird. Wenn Sie mit einer NT-Workstation arbeiten, ist diese bereits zur optimalen Zuordnung von Speicher für Anwendungen und zum Minimieren der System-Cache-Nutzung konfiguriert. Allerdings kann es ratsam sein, die Registrierung der Workstation zu überprüfen, dass LargeSystemCache den Wert 0 und nicht 1 besitzt.

Eine weitere Verringerung der System-Cache-Größe kann eventuell durch Deaktivieren des Server-Dienstes auf dem System erreicht werden. Halten Sie den Server-Dienst einfach über die Systemsteuerung an und setzen Sie die Startvariante des Dienstes auf „Deakti-

viert“. Durch diese Maßnahme wird die Möglichkeit zur gemeinsamen Verwendung von Dateien und Named Pipes auf der Maschine ausgeschaltet. Wenn also diese Funktionsmerkmale für Ihren Betrieb keine große Rolle spielen, sollten Sie diese Konfiguration einmal ausprobieren.

5 Nach der Installation von Service Pack 5 (SP5) auf meiner Windows-NT-Workstation, bekam ich Druckbenachrichtigungen und Druckbanner aus Client Services for Netware (CSNW) zu sehen. In der Systemsteuerung öffnete ich das Applet CSNW und stellte fest, dass die Bannerdruckoption (Print Banner) und die Benachrichtigungsoption bereits ausgewählt waren.
Ich löschte die Optionen und wählte sie erneut aus, aber dieser Trick funktionierte nicht. Wie kann ich meine über Novell Netware verbundenen Drucker daran hindern, Banner zu drucken?

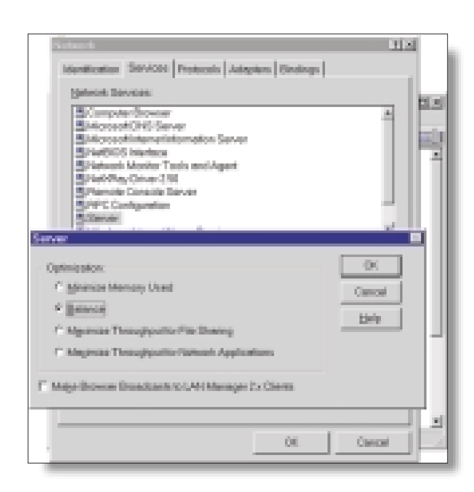


Bild 2. *Tuning der Speicherzuweisung*

SP5 ersetzt die Datei nwprovau.dll, die sich im Ordner \winnt\system32 befindet. Die neue DLL-Datei aus SP5 liest die Registrierungseinträge für Druckbanner und Benachrichtigungen von CSNW nicht richtig. Zur Lösung dieses Problems muss die SP5-Version der Datei nwprovau.dll wieder durch die SP4-Version ersetzt werden. Wenn Sie bei der Anwendung von SP5 ein Installationsverzeichnis angelegt haben, finden Sie die SP4-Version der DLL-Datei im Ordner \winnt\$ntservicepackuninstall$. Ansonsten muss die Datei von einem anderen System mit SP4 oder aus dem Ordner i386 auf der Origninal-CD-ROM von NT 4.0 kopiert werden. Falls Sie beim Versuch, die Ersatz-DLL zu kopieren, eine Meldung erhalten, dass die Datei bereits verwendet wird, besteht die einfachste Lösung darin, eine zweite Kopie von NT zu starten und die Datei dann zu ersetzen. Wenn kein zweites Betriebssystem installiert ist, können Sie ein Drittherstellerprogramm wie ERD Commander von Systems Internal verwenden, um in eine Befehlseingabeaufforderung zu booten und dann die frühere Version der Datei nwprovau.dll in den Ordner \winnt\system32 zu kopieren.

Zusammengestellt von Bob Chronister (kl)

So läuft (fast) jedes Programm als NT-Dienst

Ein Dienst für alle Fälle

von Mark Minasi

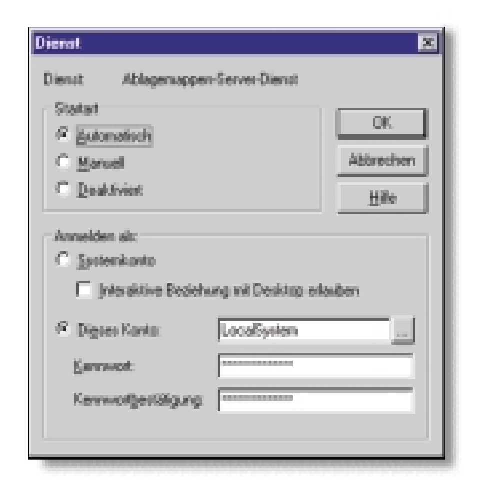
Die Dienste von Windows NT sind eine praktische Sache. Sie starten automatisch, wenn der Rechner hochfährt, laufen auch ohne angemeldeten Benutzer und nehmen keinen Platz auf dem Desktop oder der Taskbar weg. Doch nicht jedes Programm ist als NT-Dienst lauffähig. Abhilfe schafft ein kleines Werkzeug aus dem NT Server Resource Kit.

Vor allem auf unbeaufsichtigten Rechnern haben Programme, die als NT-Dienst laufen, eine Menge Vorteile. Doch damit ein Programm als Dienst ausgeführt werden kann, muss es vom Entwickler entsprechend eingerichtet worden sein. Leider ist dies oft nicht der Fall. Wäre es nicht schön, wenn auch das kleine Visual-Basic-Programm, das für die stündliche Aktualisierung einer Web-Site sorgen soll, nach jedem Reboot des Servers automatisch hochliefe, ohne dass jemand auf dem Rechner angemeldet ist, der es in Gang setzt. Es ist zwar für einen Entwickler nicht besonders schwierig, ein Programm so zu verändern, dass es als NT-Dienst läuft, doch ohne den Source-Code hat man keine Chance.

Eine Lösung bietet sich in Form des Tools srvany.exe aus dem Microsoft Windows NT Server 4.0 Resource Kit. Srvany ermöglicht es, beinahe jedes Programm als Dienst auszuführen, ohne dass das Programm erneut kompiliert werden muss. Wir möchten Ihnen in dieser und der nächsten Ausgabe die Installation und Konfiguration dieses nützlichen Werkzeugs vorstellen.

Dem Tool Srvany liegt eine raffinierte Idee zugrunde: Anstatt ein Programm als NT-Dienst neu zu kompilieren, ist Srvany selbst ein Dienst, der wiederum andere Programme startet. Srvany kann allerdings nicht alle Arten von Programmen starten. Es bleibt daher nichts anderes übrig als auszuprobieren, ob eine bestimmte Anwendung damit funktioniert oder nicht. Darüber hinaus gibt es auch Anwendungen, die nur als Dienst ausgeführt werden können, wenn ein Benutzer angemeldet ist. Bei der Abmeldung sendet NT nämlich einen Befehl an alle aktiven Programme, um ihnen diese Tatsache mitzuteilen. Viele interaktive Programme wie zum Beispiel Textverarbeitungen und Web-Browser beachten diesen Befehl und reagieren, indem sie sich selbst schließen. Solche Programme lassen sich nicht erfolgreich als Dienst betreiben.

Die Einrichtung eines Programms zur Ausführung als Dienst umfasst mehrere Schritte. Zunächst muss mit Hilfe des Tools Instsrv aus dem Resource Kit Srvany als Dienst installiert werden. Jeder Dienst besitzt einen Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services, der den Dienst beschreibt. Zum Beispiel lautet der Schlüsselname des DHCP-Server-Dienstes „DHCPServer". Srvany ermöglicht, einen Schlüsselnamen für den Dienst auszuwählen. Dies ist wichtig, da Srvany für jedes Programm, das als Dienst ausgeführt werden soll, neu installiert werden muss. Durch die Installation von Srvany unter verschiedenen Schlüsselnamen können Platzhalter für viele Programme erstellt werden, die anschließend von Srvany gestartet werden können.



Jeder NT-Dienst kann sich mit einem eigenen Benutzerkonto anmelden

Am Beispiel eines Programms notify.exe möchten wir Ihnen zeigen, wie dieses als Dienst eingerichtet wird. Dazu muss Srvany installiert und dem Dienst ein Schlüsselname wie zum Beispiel notify gegeben werden. Zum Starten von Instsrv ist in diesem Fall folgender Befehl einzugeben:

```
instsrv notify <vollständiger
_pfadname>\srvany.exe
```

Hierbei muss der vollständige Pfad zur Speicherposition von srvany.exe angegeben werden.

Wahrscheinlich müssen Sie auch das Dienstkonto für Srvany ändern. Wenn ein Benutzer ein Programm über seinen Desktop ausführt, greift das Programm auf die Daten und Berechtigungen dieses Benutzers zurück und bedient sich der entsprechenden Zugriffsrechte. Im Gegensatz dazu wird ein Dienst nicht mit den Berechtigungen und Zugriffsrechten eines Benutzers ausgeführt, sondern arbeitet mit den Rechten des Systemkontos (also LocalSystem). Dieses verfügt über umfangreiche Zugriffsmöglichkeiten auf der Workstation oder dem Server, auf dem das Konto angelegt ist, aber über praktisch keine Zugriffsautorität außerhalb der lokalen Maschine (d.h. über das Netzwerk). Dies kann bedeuten, dass der Dienst mit anderen Benutzerberechtigungen ausgestattet werden muss. Dazu öffnen Sie das Applet „Dienste" in der Systemsteuerung, wählen den Dienst aus und drücken auf „Startart". Wählen Sie im daraufhin angezeigten Dialogfeld die Option „Dieses Konto:" und geben Sie ein Benutzerkonto mit den passenden Berechtigungen an.

Wie Sie gesehen haben, ist die Einrichtung von Srvany recht einfach. In der nächsten Ausgabe werden wir anhand des Beispiels notify.exe erläutern, wie Srvany zur Ausführung eines Programms als Dienst konfiguriert wird. (fbi)

Fernreparatur vernetzter NT-Systeme

Abschied vom Turnschuh-Support

von Jonathan Cragle

Bei der Durchsicht der monatlichen Berichte Ihrer Support-Abteilung lässt sich wahrscheinlich feststellen, dass diese einen Großteil ihres Budgets darauf verwendet, Techniker zu fernen Arbeitsplätzen im gesamten Unternehmen zu senden, um Workstations zu reparieren. Ferngesteuerte Dienstprogramme zur Reparatur kleinerer Systemprobleme und zur Schulung von Benutzern stehen zwar zur Verfügung, aber wenn ein System abstürzt, muss jemand zur Reparatur entsandt werden. Abhilfe verspricht Remote Recover von Winternals Software.

Winternals Software zielt mit dem Produkt „Remote Recover" auf Systemadministratoren ab, die Remote-Systeme rasch und mit minimalem Kostenaufwand reparieren müssen. Remote Recover ermöglicht einen Zugriff auf jedes beliebige Laufwerk im Netzwerk, einschließlich NTFS- und FAT-Laufwerken sowie Laufwerken, die nicht partitioniert oder formatiert sind. Es kann sogar auf Systeme in verschiedenen Subnets der vernetzten Computerlandschaft eines Unternehmens zugegriffen werden.

Remote Recover besteht aus einer Host- und einer Client-Software-Komponente. Die Host-Software wird auf einem funktionsfähigen Windows-NT-4.0-System ausgeführt, während das System, auf dem eine Installation oder Reparatur durchgeführt werden muss, mit Hilfe der Client-Diskette gestartet wird. Diese für den Netzwerkeinsatz vorbereitete Boot-Diskette, von der ein defektes System gestartet wird, führt ein Programm aus, das kontinuierlich auf die Verbindung zu einem Host wartet, sodass kein laufendes NT-Betriebssystem auf dem Client-System notwendig ist, um Remote Recover nutzen zu können. Wenn ein Host die Verbindung zum Client hergestellt hat, zeigt Remote Recover die Laufwerke und Partitionen des Clients auf dem Host so an, als handele es sich um lokale Laufwerke. Der Host betrachtet die Laufwerke des Clients als lokal, wodurch die Ausführung von Dienstprogrammen auf niedriger Ebene, in diesem Fall auf Sektorebene, (z.B. Chkdsk, Partitionierungsprogramme, Virensucher, Datenrettungsprogramme) ausgeführt werden können. Darüber hinaus ermöglicht Remote Recover ein Kopieren von Dateien zwischen Laufwerken und sogar die Installation eines Betriebssystems auf dem Remote-Client.

Systemvoraussetzungen Remote Recover kann auf jedes Laufwerk zugreifen, das die Schnittstelle für Interrupt 13 (INT 13) unterstützt. INT 13 ist Teil des BIOS eines Computers, das den Zugriff auf eine Systempartition ermöglicht. Um festzustellen, ob ein Laufwerk INT 13 unterstützt, kann der Befehl Fdisk /status von einer bootfähigen DOS-Diskette aus ausgeführt werden. Wenn Fdisk das Laufwerk korrekt lesen kann, ist Remote Recover in der Lage, auf das Laufwerk zuzugreifen.

Zur Erstellung der Client-Diskette wird die NDIS2-(Network-Device-Interface-Specification-2-)Treiberschnittstelle von Microsoft verwendet. Es muss ein NDIS2-Treiber für die von den Clients benutzte Netzwerkkarte (NIC) vorhanden sein, da die Clients ansonsten keine Verbindung zum Remote-Recover-System herstellen können (d.h., NDIS3-Treiber funktionieren nicht). In der Regel stehen NDIS2-Treiber auf der Diskette oder der CD-ROM zur Verfügung, die mit der NIC geliefert werden.

Testumgebung Zur Beurteilung von Remote Recover wurden zwei vernetzte Systeme eingesetzt: Ein System diente als Host, das andere als Client. Remote Recover wird in einer komprimierten ZIP-Datei geliefert, die auf den Recover-Host kopiert wurde. Die Installation ist sehr einfach. Remote Recover wurde über das Startmenü geöffnet und die Option zur Erstellung einer Client-Diskette im Dateimenü ausgewählt. Dann

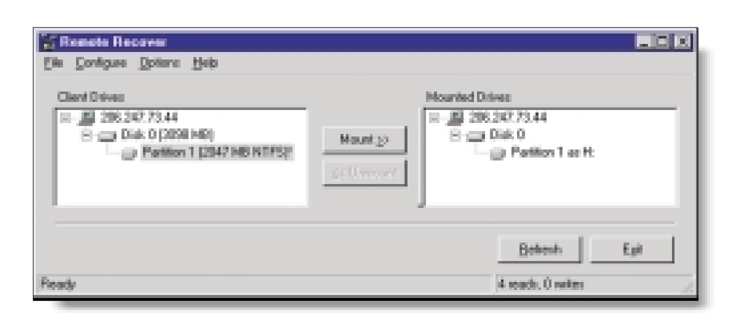


Bild 1. *Mounten ferner Laufwerke mit Hilfe des Hosts von Remote Recover*

wurde eine bootfähige MS-DOS-Diskette in das Host-Testsystem eingelegt. Das System forderte den Tester auf, eine NT-Server-4.0-CD-ROM einzulegen und durch Klicken durch die Menüs das Verzeichnis MSCLIENT zu öffnen. Als Nächstes forderte die Software den Tester zur Eingabe einer IP-Adresse, einer Subnet-Maske und einer Gateway-Adresse auf, die vom Client-System zum Starten verwendet werden, sodass der Host den Client lokalisieren kann. Wenn mit DHCP gearbeitet wird, muss sichergestellt werden, dass die für die Client-Diskette angegebene IP-Adresse nicht mit bereits verwendeten statischen Adressen in Konflikt gerät. Die Erstellung der Client-Diskette dauerte weniger als eine Minute und wurde gleich anschließend in das Client-Testsystem eingelegt.

Mit Hilfe der neu erstellten Boot-Diskette wurde das Client-System gestartet, während auf dem Host-System Remote Recover aufgerufen wurde. Wie in Bild 1 zu erkennen ist, wurde die Einzelpartition gemounted und Partitionmagic von Powerquest auf dem Host-System geöffnet. Dann wurde das Client-Laufwerk ausgewählt und eine 2-GB-Partition erstellt und formatiert. Die Arbeit mit dem Laufwerk des Clients gestaltete sich problemlos: Dateien wurden hinzugefügt und gelöscht, eine Virensuche durchgeführt und die Registrierung des Laufwerks und andere wichtige Dateien gesichert. Nach Beendigung des Tests wurden die Client-Laufwerke aus der Remote-Recover-GUI auf dem Host-System entfernt.

Beim Kopieren eines gesamten Laufwerks ist die Partition, die kopiert werden soll, zu berücksichtigen, da keine Partition auf einem System kopiert werden kann, die zur Zeit in Gebrauch ist. Um diese Einschränkung zu umgehen, kann im Host-System ein Laufwerk – das NT Server oder NT Workstation enthält – installiert, das Laufwerk mit dem Client-Laufwerk – das kopiert werden soll – gemounted und die Host-Partition dann auf den Client kopiert werden. Alternativ kann auch eine Partition von einem anderen Client-System kopiert und auf einer neuen Festplatte installiert werden. Wenn auf eine dieser Möglichkeiten zurückgegriffen wird, muss das Microsoft-Dienstprogramm „Sysprep“ zur Systemvorbereitung beim Kopieren der Partition verwendet werden, um zu gewährleisten, dass die SID des Host und die SID des Clients sowie die Host-Namen unterschiedlich sind.

Fazit Anwender werden zu schätzen wissen, wieviel Geld Remote Recover bei der Remote-Installation eines Betriebssystems oder beim Reparieren einer fernen Workstation einsparen hilft, ohne den eigenen Schreibtisch dazu zu verlassen. Dieses Produkt ermöglicht gleichermaßen einfache und komplizierte Systemreparaturen und distanziert durch seine Leistung die Konkurrenz. Remote Recover ist sehr empfehlenswert und für den Preis in Anbetracht der zahlreichen Nutzungsmöglichkeiten beinahe geschenkt. Eine Testkopie von Remote Recover steht auf der Web-Site von Winternals Software (http://www.winternals.com) zum Download bereit. (kl)

Remote Recover

Hersteller:
Winternals Software
Tel. 001 512-330-9861

Anbieter:
Globalsoft
Tel. 030/74374775

Preis:
595 Mark pro Benutzerlizenz (bis vier Lizenzen)

Systemanforderungen:
- Windows NT Server 4.0 oder NT Workstation 4.0
- Startdiskette für MS-DOS 4.0 oder spätere Version bzw. Windows 9x
- NDIS2-Treiber
- Für INT 13 zugängliche IDE- oder SCSI-Festplatte

Web-Links und Info-Anforderung unter www.win2000mag.de/info

Kostengünstige Replikation von Dateien

Doppelt hält besser

von Marty Scher

Im Falle eines Server-Verlusts ist für viele Organisationen die Verfügbarkeit kritischer Dateien äußerst wichtig. Meist gibt es archivierte Dateien, aber stehen diese auch vor Ort zur Verfügung? Und wie lange wird die Wiederherstellung archivierter Dateien dauern? Wohl dem, der seine Daten auf einem gespiegelten Server redudant vorhält.

Datenreplikation ist eine wichtige Technologie, die gerade zur richtigen Zeit verfügbar sein muss. Viele Replikationsprodukte bieten Lösungen durch Hardware-Clustering an, die sich auf teure Hardware-Komponenten und Add-ons für das Betriebssystem stützen. „Suresync Real-Time“ von Software Pursuits ist hingegen eine Software-Lösung zur Replikation und Spiegelung von Dateien.

Im Test wurde Suresync Real-Time auf Servern unter Windows 2000 Server (Win2K Server) Beta 3 installiert. Die Installation war einfach und verlief — bis auf einen kleineren Fehler im Zusammenhang mit einem Aufruf an ole2.dll — ohne besondere Vorkommnisse. Die Fehlermeldung besagte, dass das System auf diese Datei nicht zugreifen konnte, jedoch wirkte sich der Fehler weder auf die Installation noch auf den allgemeinen Betrieb des Produkts

aus. (Der technische Support von Software Pursuits ist dabei, den Fehler auszuwerten.) Aber in Anbetracht der Tatsache, dass bei dem Software-Einsatz auf einer Betaversion eines Betriebssystems nur eine Störung auftrat, gestaltete sich der Betrieb des Produkts problemlos und intuitiv. Die Installationsoptionen des Produkts zur lokalen Installation und zur Netzwerkinstallation vereinfachen die Installation auf weiteren Servern.

Die Konfiguration der Software war ebenso einfach wie die Installation. Zur Replikation von Dateien zwischen zwei oder mehr Systemen wird eine Anzahl von Methoden oder Regeln verwendet, die festlegen, wann und wie Dateien durch das Produkt aktualisiert werden. Suresync Real-Time kann geöffnete Dateien verarbeiten und erzwingt das Schließen einer geöffneten Datei, falls dies notwendig ist.

Software Pursuits hat das angekündigte Ziel, ein Produkt zu schaffen, für das kein Benutzerhandbuch erforderlich ist, beinahe erreicht. (Dennoch ist dem Produkt ein umfangreiches gedrucktes Handbuch beigefügt.) Zum Beispiel führen Assistenten durch die einzelnen Einstellungen zur Erstellung einer neuen Relation (die Bezeichnung in Suresync Real-Time für die Konfiguration einer Dateireplikation). Bild 1 zeigt die Auswahlmöglichkeiten für die Konfiguration einer neuen Relation. Die Assistenten bieten auch die Möglichkeit zum Testen einer Relation. Die umfassende Online-Hilfe bietet Antworten auf die meisten Fragen zur Konfiguration. Beim ersten Versuch, eine Relation einzurichten, wählte der Tester die Optionen zur Spiegelung freigegebener Ordner auf zwei Servern nach eigenen Vermutungen aus. Das Ergebnis war einerseits eine Meldung, dass die Konfiguration erfolgreich war, aber andererseits auch eine Fehlermeldung, die auf einen Lizenzfehler für Suresync Real-Time hinwies. Anhand der Online-Hilfe konnte geklärt werden, dass in diesem Fall eine Workstation-Lizenz unter Windows NT Server verwendet wurde. Der Fehler wurde durch Hinzufügen der richtigen Lizenz beseitigt.

Suresync Real-Time verfügt über einen robusten Zeitplandienst, der nützlich ist, um während der Zeiten geringerer Systemauslastung eine Replikation über WAN-Verbindungen und andere langsame Verbindungen durchzuführen.

Da Administratoren die meisten Aufgaben in Echtzeit erledigen, wurden die Echtzeit-Replikationsfunktionen der Software getestet. Dazu konfigurierten wir eine Testrelation zur Spiegelung von zwei Freigaben. Anfangs fügt das Programm dem Hauptordner (Master), d.h. dem Quellordner, einige Textdateien hinzu. Wenn Suresync Real-Time eine hinzugefügte Datei erkennt, repliziert das Programm die Datei an die Zielposition. Die Änderungen benötigten konstant zwischen 50 und 55 Sekunden zur Replikation. Dies ist zwar ein recht achtbares Ergebnis, jedoch nicht unbedingt Echtzeit. Eine prompte E-Mail-Nachricht vom technischen Support erläuterte, dass die Replikationszeiten durch Ändern der Synchronisierungspriorität (von normal) auf hoch verringert werden können.

Nach dem Ändern der Synchronisierungspriorität wurden die aktualisierten Dateien rasch repliziert. Für den Test wurde ein Skript erstellt, das willkürlich benannte und unterschiedlich große Dateien generierte. Das Programm replizierte die zusätzlichen Dateien beinahe ebenso schnell wie sie generiert wurden. Andere Relationen wie zum Beispiel der Peer-zu-Peer-Austausch von Kopien („Exchanging Copies") funktionierte ebenfalls einwandfrei. Bei dieser Art der Relation sind mehrere Kopien einer Datei an mehreren Speicherpositionen vorhanden. Wenn eine der Kopien geändert wird, repliziert das Programm die Änderungen zu allen anderen Kopien.

Suresync Real-Time ist ein robustes und gut entwickeltes Produkt. Darüber hinaus ist das Produkt recht vielseitig. Es bietet zum Beispiel verschiedene Methoden zur Replikation von Datendateien an. Zudem verfügt die Software über verschiedene Funktionen zur Ereignisprotokollierung sowie zur Generierung von E-Mail-Warnungen. Suresync Real-Time ist gewiss aller Beachtung wert. (kl)

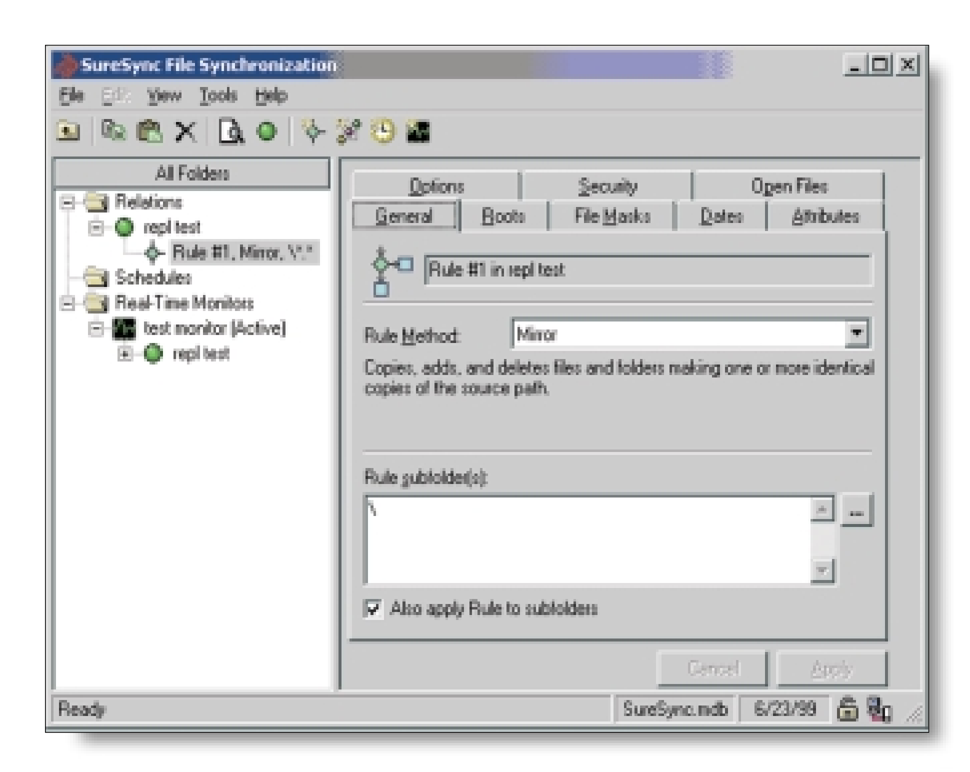


Bild 1. *Konfigurieren einer Regel mit Suresync File Synchronization*

Suresync Real-Time

Hersteller:
Software Pursuits
Tel. 001 650 3720900 oder
001 800 3674823

Preis:
159 Dollar pro Benutzer

Systemanforderungen:
- 486er Prozessor oder besser
- Windows NT 4.0
- 16 MB RAM
- 20 MB Festplattenspeicher

Web-Links und Info-Anforderung unter www.win2000mag.de/info

NT-Administrationswerkzeuge mit MMC-Integration

Eine Fundgrube für gestresste Administratoren

von Tom Henderson

Aelita Enterprise Suite (AES) 2.04 ist eine Sammlung von Dienstprogrammen und administrativen Erweiterungen, die die Assistenten und Anwendungen zur Verwaltung und Systemsteuerung von Windows NT aufstocken. Dieser Satz von Dienstprogrammen erweitert die Microsoft Management-Konsole (MMC) des NT-4.0-Option-Pack um Funktionen u.a. zum Management von Domänenbeziehungen, zur Erstellung von Berichten über Benutzer und Berechtigungen sowie zum Ereignismanagement.

Die fünf Minuten dauernde Installation gestaltet sich recht einfach. Für den Test wurde ein sauberer Server unter NT 4.0 mit Service-Pack 5 (SP5) verwendet. Die Standardeinstellungen für die Dateipositionen funktionierten reibungslos. Die Software bietet dem Benutzer verschiedene Anwendungen und Dienstprogramme an: Aelita Delegation Manager (Aelita DM), Domain Migration Wizard (DMW), Virtuosity, Journal, Eventadmin, Bootadmin, Erdisk, Multireg und Timeadmin*.

Die Software-Suite AES 2.04 enthält außerdem das Administrator-Assistant-Tool-Kit, in dem drei weitere Dienstprogramme enthalten sind. Nach der Installation war nicht gleich klar, wie die Anwendungen zu starten waren, weil die Programmserie über keine Steueranwendung verfügt, mit deren Hilfe die getrennten Anwendungen und Dienstprogramme gestartet werden können. Zudem gibt es keine Readme-Datei zur Software, sodass die Antwort in der etwas spärlichen Online-Hilfe gesucht werden musste.

Aelita DM ist ein Tool, mit dem die Sicherheit von NT-Domänen und Mitglieds-Servern und Workstation verwaltet wird. Der Zweck des Tools besteht darin, Administratoren von Subdomänen, die keine administrative Kontrolle über die gesamte Domäne benötigen, mit Sicherheitsberechtigungen auszustatten. Ohne Einzelbenutzer zu Mitgliedern der Administratorengruppe zu machen, können Administratoren mit Hilfe von Aelita DM einzelnen Benutzern Berechtigungen zur Ausführung bestimmter Aufgaben erteilen. Man kann zum Beispiel Subdomain-Administratoren die Möglichkeit geben, gesperrte Konten wieder zu aktivieren wie in Bild 1 zu sehen ist.

Mit dem **Domain Migration Wizard** werden Abbildungen auf NDS-Partitionen durchgeführt, und es kann die Hierarchie von Active Directory (AD) unter Windows 2000 (Win2K) verwaltet werden. DMW ist für Administratoren nützlich, die Systeme von NT auf Win2K umstellen müssen. Dieser Assistent ist eine Art Werkzeugkasten, der bei der Migration von NT-Domänen auf das hierarchische AD-Modell behilflich ist. Zum Testen der Features von DMW wurden mehrere zusätzliche Server zur Herstellung eines Szenarios mit mehreren Hauptdomänen installiert. Der Vorgang als solcher war einfach, jedoch konnte bzw. musste unter zahlreichen Optionen ausgewählt werden, zum Beispiel, um festzulegen, welche Organisationseinheiten zu migrieren waren und welche Benutzernamen aufgelöst werden sollten. Im folgenden Test wurden Informationen aus der NT-4.0-Domäne in Windows 2000 Advanced Server (Win2K AS) Release Candidate 2 (RC2) umgestellt, ohne die ursprüngliche NT-Konten- und Gruppeninformationen zu entfernen. DMW bietet die Möglichkeit, alle Domänen zu öffnen und anschließend Objekte und Gruppen einfach zusammenzuziehen. Diese Anwendung funktionierte im Testnetzwerk gut, allerdings war das Testnetzwerk nicht groß genug, um alle Vorteile zu testen, die diese Anwendung einem großen Netzwerk bietet.

DMW stützt sich weitgehend auf **„Virtuosity“**; diese Anwendung sammelt Berechtigungen, Benutzer, Profile sowie Domänen- und andere Daten und fügt die Daten in die enthaltenen Microsoft Access- und Microsoft-Jet-Datenbanken ein (mit einigen Feineinstellungen kann auch eine ODBC-Datenbank verwendet werden). Es können vorgefertigte und benutzerdefinierte Berichte über die Daten generiert werden, die von Virtuosity aus Domänen, Servern und PCs gesammelt werden. Die Berichte enthalten Elemente wie einfache statistische Beziehungen, ungeeignete Benutzernamen sowie Dateien, die in einem bestimmten Zeitraum geändert wurden. Da dieses Tool eine große Menge an Daten verarbeitet, kann die Generierung eines Be-

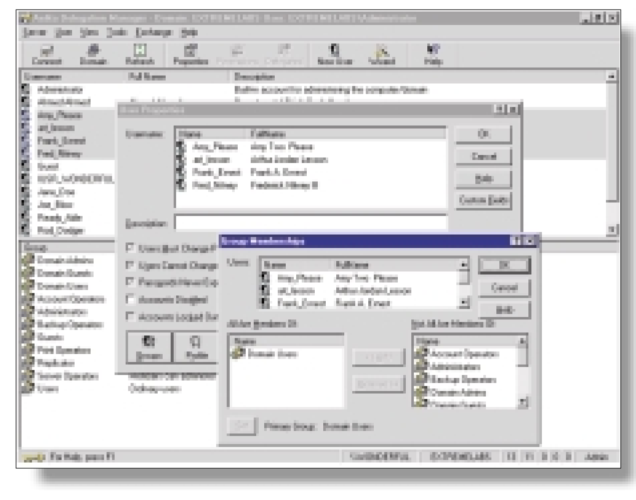


Bild 1. *Erteilen von Berechtigungen mit Hilfe von Aelita DM*

richts über ein großes Netzwerk geraume Zeit in Anspruch nehmen.

Journal ist ein Zeitplandämon, mit dessen Hilfe die Datensätze, die von anderen Anwendungen gespeichert werden, mit verschiedenen Differenzierungsgraden analysiert werden können. Journal bietet die Möglichkeit, als autonomer Agent für Administratoren ausgeführt zu werden, wie in Bild 2 zu sehen ist. Nach der Durchführung einer Analyse kann Journal so konfiguriert werden, dass eine Abfrage, eine Anwendung oder ein Messaging-System (z.B. E-Mail, Pager, SNMP-Trap) zur Verfolgung von Ereignissen gestartet werden kann. Unterschiedliche Ergebnisse der Ereignisanalyse können unterschiedliche Anwendungen bzw. E-Mail-Adressen ansprechen. Auf diese Weise ermöglicht Journal eine Verfolgung zahlreicher Ereignisse. Diese weitreichenden Differenzierungsmöglichkeiten sind zwar oft nicht notwendig, aber manch einer wird diese Optionen zu schätzen lernen. Mit Hilfe von Journal kann festgestellt werden, wann eine Analyse zum letzten Mal ausgeführt wurde. Anschließend kann über Journal der entsprechende Bericht angezeigt werden. Die im Test erstellten Berichte waren recht vollständig, sodass sich eine weitere Suche in Access erübrigte.

Eventadmin ist ein Repository und Aktionsagent (Benachrichtungsagent) für netzwerkweite NT-Ereignisse, die von Journal gesammelt werden. Eventadmin verfolgt solche Ereignisse wie ungültige Anmeldeversuche, fehlgeschlagene Dateizugriffe und Dr.-Watson-Fehler. Darüber hinaus zeichnet die Anwendung Server-Ereignisse im Event Viewer auf. Die Ereignisse können leicht sortiert werden, jedoch gibt die Anwendung keine Hilfestellung bei der Interpretation der aufgezeichneten Daten.

Im Test wurden einige Ereignisse erstellt, die Eventadmin melden konnte. Die Anwendung wurde so konfiguriert, dass sie E-Mail-Nachrichten an den Tester schickte. Eventadmin verfolgt mehrere Server, um Berichte zu Anwendungs-, Sicherheits- und Systemereignissen zu generieren. Zur Sicherheitsanalyse können in die Berichte Elemente wie zum Beispiel Datei- und Objektzugriff, Anmeldestatus, Anmeldezeiten, Änderungen an Gruppen, Informationen zu neuen Konten, Änderungen an Sicherheitsrichtlinien sowie Benutzeraktivitäten aufgenommen werden. Es können außerdem Berichte über Drucker, über die Festplattenkapazität, RAS und Speichermanagement generiert werden. Wie bei den meisten AES-Anwendungen kann mit Hilfe des Scheduler Wizard die Anwendung Eventadmin zeitlich so eingestellt werden, dass Berichte

Aelita Enterprise Suite 2.04

Hersteller:
Aelita Software Group

Anbieter:
GlobalSoft
Tel. 030-743 747 75

Systemanforderungen:
◆ Windows NT 4.0 oder NT 3.51

Web-Links und Info-Anforderung unter www.win2000mag.de/info

zu einem bestimmten Zeitpunkt ausgeführt werden.

Die übrigen AES-Anwendungen besitzen eine etwas eingeschränkte Funktionalität. Zum Beispiel dient **Bootadmin** lediglich dem einzigen Zweck, das Remote-Herunterfahren und -Neustarten von Rechnern in einer Domäne zu erzwingen. Mit Hilfe von Bootadmin können Anwendungen zum Schließen mit ungesicherten Änderungen konfiguriert, Neustarts nach Herunterfahren durchgeführt, unterschiedliche Warnnachrichten zur Anzeige vor dem Herunterfahren festgelegt und Ereignisse in einer Protokolldatei aufgezeichnet werden. Außerdem kann Bootadmin auch zur Ausführung nach einem vorbestimmten Zeitplan konfiguriert werden. Diese Anwendung funktionierte im Test reibungslos.

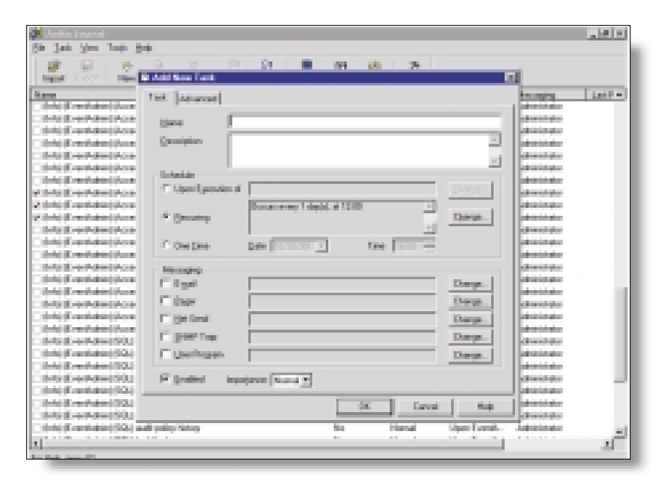


Bild 2. *Konfigurieren eines Tasks in Journal*

Das Dienstprogramm **Erdisk** erstellt und speichert Notfalldisketten (Emergency Repair Disks – ERDs) für NT-Server und NT-Workstations und speichert den Inhalt der Notfalldisketten in einem Verzeichnis, das dazukonfiguriert wird. (Aelita empfiehlt, Notfalldisketten in einem nicht zugänglichen Bereich zu speichern, um Eindringlinge am Zugriff auf die Registrierungs- und Sicherheitsdaten zu hindern, die auf den Notfalldisketten enthalten sind.) Im Test wurden Notfalldisketten für die fünf Server erstellt und die Inhalte der Notfalldisketten ohne besondere Vorkommnisse auf einem PDC gespeichert. Die Ausführung von Erdisk kann mit Hilfe des Scheduler Wizard in Gang gesetzt werden. Erdisk mangelt es jedoch an einer Methode zur Erstellung von Notfalldisketten für Windows 9x-Maschinen.

Multireg ist ein Dienstprogramm, mit dessen Hilfe ein COM-Element auf die Registrierungsschlüssel mehrerer NT-Maschinen gleichzeitig zugreifen kann. Dieses Tool arbeitet mit der gleichen Benutzerschnittstelle (UI) wie Regedit. Mit diesem Tool können Registrierungsschlüssel unter einer Gruppe von Maschinen zur Umsetzung von Richtlinien synchronisiert, Microsoft-Office-Anwendungen verankert oder Virusänderungen verhindert werden. Mit Hilfe von Journal können Änderungen an Registrierungsschlüsseln überwacht, erkannt und untersucht werden. Im Test wurde die Anwendung Multireg geöffnet und ein System als Basissystem ausgewählt. Nach einer Änderung auf dem Basissystem wurde diese Änderung von Multireg automatisch auf die anderen Systeme repliziert, die zuvor ausgewählt worden waren. Allerdings können auch alle Server in einer einzigen Aktion außer Gefecht gesetzt werden. Daher sollte Multireg unbedingt unter Verschluss gehalten werden.

Die Anwendung **Timeadmin** dient lediglich zur Aktualisierung von Servern, um die Systemzeiten zu synchronisieren. Die Systemzeiten können mit Hilfe des Zeitplanassistenten (Scheduler Wizard) synchronisiert werden. Der Zeit-Server, den Aelita als Standardzeitquelle gewählt hat, ist nur schwer zu erreichen, aber es können andere Zeit-Server weltweit ausgewählt werden (z.B. http://www.time.nist.gov, http://www.nist1.datum.com). Zahlreiche Firewalls blockieren Port 13, der vom Network-Time-Service verwendet wird, sodass eventuell ein Proxy durch die Firewall eingesetzt werden muss, wie dies im Test der Fall war. Timeadmin erweitert die gewöhnlich eingeschränkten Zeitsynchronisierungsfunktionen, die verschiedene Freeware-Anwendungen anbieten, um eine Protokollfunktion sowie um eine zentrale Verwaltung.

Und schließlich enthält das **Administrator-Assistant-Tool-Kit** die Programme Fileadmin, Regadmin und Scanpro. Mit Hilfe von Fileadmin können Administratoren Berechtigungen für Ordner, Dateien oder Dateigruppen hinzufügen, entfernen, ändern oder klonen. Anschließend können die Änderungen in einer ganzen Verzeichnisbaumstruktur repliziert werden, ohne die Berechtigungsattribute für andere Konten zu ändern. Das Tool Regadmin, das dem Programm Regedit ähnelt, ermöglicht ein Klonen, Kopieren und Replizieren von Registrierungsstrukturen oder -einträgen. Bei der Bearbeitung von Registrierungseinträgen bietet dieses Tool einfachere Möglichkeiten zur Veränderung von Strukturen und Werten, als dies in Regedit bewerkstelligt werden kann. Ebenso wie für Multireg gilt auch für Regadmin, dass mit diesem Tool ein Server mit einem Schlag lahmgelegt werden kann, sodass besondere Vorsicht beim Einsatz geboten ist. Scanpro ist ein interessantes Dienstprogramm, das zum Testen von Kennwörtern gegen Wörterbuchangriffe eingesetzt werden kann. Auch wenn dem Wörterbuch Wörter hinzugefügt werden können, ist die Standardversion recht klein. Im Test wurden verschiedene englische Wörter verwendet, die Scanpro nicht im Wörterbuch als Kennwörter hatte, sodass das Tool sie spielend umging. Das Durchsuchen des Wörterbuchs nach dem Kennwort eines Benutzers auf einem 366-MHz-Server nahm neun Sekunden in Anspruch. Ein größeres Wörterbuch würde eine längere Zeit zum Testen eines Kennworts benötigen, böte aber auch eine realistischere Simulation eines Wörterbuchangriffs. Scanpro kann leicht mit einem Zeitplaner terminiert werden. Mit dem Tool können Server und Domänen regelmäßigen Überwachungsoperationen unterzogen werden, um sicherzutellen, dass neue Kennwörter gegen Angriffe gefeit sind.

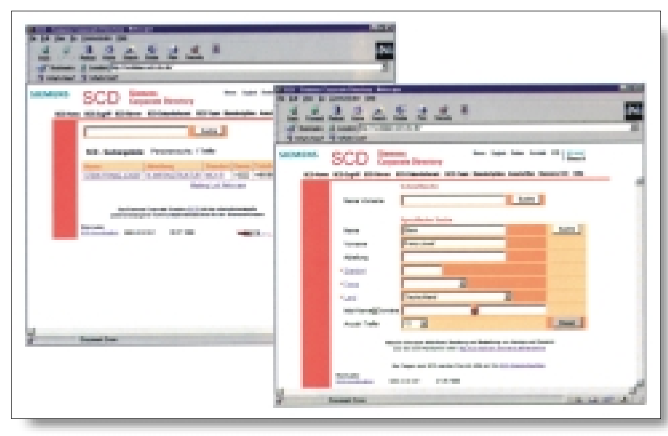
AES ist sehr nützlich, besitzt jedoch noch einige Ungeschliffenheiten. Aelita müsste die Online-Hilfe ausbauen und weitere Assistenten und Vorlagen zur Verfügung stellen, um Administratoren eine leichtere Handhabung der Suite zu bieten. Darüber hinaus könnte die Software davon profitieren, wenn alle Komponenten unter einer Shell-Anwendung zusammengefasst würden. AES unterstützt Administratoren, die mit der Pflege mittelgroßer oder für ganze Unternehmen ausgebauter NT-Netzwerke betraut sind.

* Der Begriff Timeadmin ist in Deutschland sowie in den anderen EU-Staaten ein geschützter Begriff des deutschen Software-Unternehmens N.T.K.M. Seit Sommer letzten Jahres gab es deswegen Verhandlungen mit Aelita. Die Funktion des Programmes Timeadmin ist mittlerweile aber ein wesentlicher Bestandteil von Windows 2000. Timeadmin von Aelita hat sich so gesehen daher überlebt. (Anm. der Redaktion) (kl)



Siemens-Meta-Directory DirX mit Windows-2000-Support

Auf der CeBIT hat der Siemens-Bereich Information and Communication Networks die neue Version 5.5 von „DirX Meta Directory“ vorgestellt. Der Verzeichnisdienst unterstützt nun durchgängig das Sicherheitsprotokoll SSL/TLS für eine geschützte Datenübertragung. Funktionserweiterungen stellen dabei den Zugriff auf Verzeichnisse von SAP R/3 HR, Novell NDS, Microsoft Windows 2000 sowie Siemens DS-WIN/Hicom DMS sicher. Die DirX Meta-Directory-Produktfamilie besteht aus vier Komponenten. Der **Directory-Server DirX** ist LDAP-v3-kompatibel und basiert auf dem X.500-Standard. DirX dient hauptsächlich der Datenhaltung für unternehmensweite Meta-Directories. Neben Windows NT, Linux und verschiedenen anderen Unix-Plattformen unterstützt DirX in Version 5.5 auch Windows 2000.



DirXweb verbindet den DirX-Server mit Standard-Internet- oder Intranet-Web-Servern

Mittels **DirXmetahub** wird DirX zum globalen Verzeichnisdienst, der über die so genannten Meta-Agenten andere im Unternehmen vorhandene Benutzerverzeichnisse zu einem einzigen globalen Verzeichnis zusammenführt.

Das Meta Directory erzeugt mit Hilfe von Synchronisations- und Replikationswerkzeugen ein logisch einheitliches, unternehmensweit verfügbares Directory. Der LDAP-Client, **DirXdiscover** ermöglicht die Suche, Pflege und Verwaltung von Daten in DirX und angeschlossenen LDAP-Directories. Bei Einsatz des DirX-LDAP-Servers erlaubt DirXdiscover überdies Single-Sign-On für NT. **DirXweb** verbindet den DirX-Server mit Standard-Internet- oder Intranet-Web-Servern. Der Zugriff auf die Directory-Daten erfolgt über einen Standard-Browser. Benutzer haben somit die Möglichkeit, Daten in LDAP- oder X.500-Directories mit LDAP-Zugang abzufragen und zu administrieren. DirXweb unterstützt in Verbindung mit dem DirX-LDAP-Server ebenfalls Single-Sign-On für NT. (kl)



Siemens
Tel.: 089/722-47228
www.siemens.de

Datenverfügbarkeit für Windows 2000

Auf der CeBIT hat Legato die Unterstützung der Windows-2000-Plattform mit einem umfangreichen Software-Paket für den Schutz von kritischen Daten und Anwendungen in Betriebsumgebungen demonstriert. Es reicht von der Standard-Datensicherung von Servern in einzelnen Abteilungen bis hin zu umfassender „Information Continuance“ in anspruchsvollen Umgebungen wie z.B. für E-Commerce.

Zu den ersten Legato-Produkten, die Windows 2000 unterstützen, gehören

- die Networker-Backup- und Recovery-Software für den Schutz unternehmenskritischer Daten,
- die neue Datenreplikations-Software „Octopus“ für das Disaster Recovery sowie
- „Legato Cluster Enterprise“ für die Hochverfügbarkeit von Anwendungen in Windows-2000-Systemen.

Der Legato Networker bildet die Grundlage der Software-Produkte von Legato für SANs. Mit dem Networker können Organisationen die Daten in ihren kritischen, Windows-2000-basierten Systemen mit einer unkomplizierten und integrierten Lösung schützen. Der Legato Networker bietet einen stabilen und zuverlässigen Datenschutz durch Medienmanagement-Technologien für fehlerfreies und automatisiertes Backup und Recovery aller Unternehmensdaten – sowohl in SANs als auch in traditionellen Speicherumgebungen.

Legato zeigte auch die Octopus-4.0-Datenreplikations-Software und Celestra, die neue Technologie für das Server-lose Backup auf Windows NT. (kl)

Legato Systems
Tel.: 089/8996920
www.legato.com

Mit Groupwise zum E-Business

Auf der CeBIT hat Novell jetzt Details der neuen Version von Groupwise vorgestellt. Groupwise stellt Unternehmen als universelle Wissensplattform eine breite Palette an Net-Services-Software zur Verfügung: Messaging, ein integriertes Zeitplansystem, Dokumentenmanagement und Workflow-Funktionen. Die neue Version mit dem Codenamen „Bulletproof“ ergänzt das Portfolio von Novells Net-Services-Software und erweitert die Funktionalität von Groupwise über alle Typen von Netzwerken und wichtigen Betriebssysteme hinweg. Die wichtigste Neuerung von „Bulletproof“ ist die integrierte XML-Infrastruktur, die eine vollständige und einfache Einbindung von Produkten und Diensten Dritter gestattet. Dazu gehören beispielsweise Virus-Scanner und Workflow-Applikationen. So können auf Basis des Groupwise-Systems komplette Netzlösungen erstellt werden, die alle bestehenden Netze integrieren.

Weitere Verbesserungen finden sich vor allem in den folgenden Kernbereichen: Hohe Zuverlässigkeit und Skalierbarkeit, plattformunabhängiger Zugriff, Systemmanagement und Sicherheit. Zusammengenommen erlauben die Erweiterungen dem Benutzer zu jeder Zeit und von jedem Ort aus den einfachen Zugriff auf relevante Informationen. So wird es möglich, Unternehmensprozesse einfach auf das Internet auszuweiten und dort Geschäfte zu tätigen. Die „Bulletproof“-Version soll Ende diesen Jahres verfügbar sein. (kl)

Novell
Tel.: 0211/5631-3661
www.novell.de



Komplettes Recovery

Auf der CeBIT zeigte Veritas ihre Backup-Software für Microsoft Windows 2000 Server/Advanced. „Backup Exec 8.0“ unterstützt Backup und Recovery für alle Komponenten von Windows 2000 wie Active Directory, File System 5.0 sowie weitere Features wie Encrypted File System und Distributed File System. Anwender erhalten damit zusätzlich zu der in Windows 2000 enthaltenen Backup-Utility eine robuste Speicherlösung für ihre Windows-NT/2000-Umgebung. Microsoft Windows NT 4 wird von Veritas Backup Exec 8 ebenfalls unterstützt.

Ein neuer Scheduler in Kalenderform erleichtert die Planung von Backup- und Recovery-Jobs mit Berücksichtigung von Feiertagen und Urlaubszeiten. Erweitert wurde der integrierte Virenschutz: Veritas Backup Exec prüft vor dem Sichern auch komprimierte Dateien auf ihre Integrität. Die Intelligent-Disaster-Recovery-Option bietet jetzt komplettes Recovery für Dateien unter Windows 2000 und Windows NT. Darüber hinaus unterstützt Veritas Backup Exec automatisches Failover in Microsoft-Cluster-Umgebungen. Über eine beliebige Windows-2000/NT-Konsole lässt sich mit der neuen Option Network Storage Executive eine Vielzahl von Backup-Exec-Servern im Unternehmen von einer zentralen Konsole verwalten. (kl)

Veritas Software
Tel.: 069/95 09-61 88
www.veritas.com

Lösungsorientierte Angebote

Unter dem Motto „Networks of Confidence“ präsentierten die Divisions und Business Units der Gruppe Bull in diesem Jahr auf der CeBIT eine Reihe von Lösungen, die die Abstimmung von Informationssystemen und Software auf die individuellen Anforderungen des Unternehmens und seiner Kunden gewährleisten sollen. Der Schwerpunkt des diesjährigen Messeauftritts der Servers Division lag dementsprechend mehr in der Technologieberatung als in der Präsentation von Hardware-Produkten.

Auf einem der ersten Systeme, die auf der neuen IA-64-Architektur von Intel mit dem Itanium-Prozessor als Herzstück basiert, wurde Microsofts SQL-Server mit der 64-Bit-Version von Windows 2000 und einer Anwendung des so genannten „Terraservers“ gezeigt. Die neue IA-64-Server-Familie des Unternehmens soll ab Mitte dieses Jahres verfügbar sein. Bull unterstützt die 64-Bit-Version von Windows 2000 als eines der strategischen Betriebssysteme für seine IA-64-Plattformen. Als Front-Line-Partner von Microsoft hat die Bull-Gruppe die offizielle Vorstellung von Windows 2000 zum Anlass genommen, eine OEM-Vereinbarung mit dem Software-Hersteller anzukündigen. Auf der Familie der Express5800-Server und der IA-64 Itanium-Plattform soll in Zukunft Windows 2000 vorinstalliert werden. (kl)

Bull
Tel.: 0 22 03/30 50
www.bull.de

Durchgängige VPN-Lösung von NCP

Eine durchgängige Lösung für die Einrichtung Virtueller Privater Netzwerke (VPN) über das Internet stellte der Nürnberger Hersteller NCP Engineering vor. Mit VPNs ist es möglich, sichere Verbindungen zwischen zwei Rechnern über die Infrastruktur des Internets aufzubauen. Hierzu wird eine gesicherte Datenübertragung über einen so genannten „Tunnel“ implementiert.

Die Besonderheit der NCP-Lösung: Im Gegensatz zu IPSec-basierenden Lösungen implementierte NCP das komplette Security-Management in das Point-to-Point-Protokoll PPP, also im OSI-Layer 2. Auf Basis des SSL-Protokolls erfolgen sowohl die Verhandlung der Session Keys als auch die Authentifizierung der Kommunikationsparter über Zertifikate nach X.509v3. NCP nennt diese Kombination von PPP mit SSL „L2Sec“.

Die VPN-Lösung von NCP bietet, anders als IPSec-basierende Verbindungen, eine völlige Unabhängigkeit von der verwendeten Telekommunikationsumgebung. Der Tunnel wird zwischen VPN-Client und dem VPN-Gateway in der Firmenzentrale aufgebaut. Die kompletten IP-Datenpakete (sowohl IP-Header als auch Nutzdaten) werden verschlüsselt und mit einem neuen Header versehen. Damit können zwischen den beiden Endpunkten des Tunnels beliebig viele Router installiert sein, die selbst weder über Verschlüsselungs- noch Tunneling-Funktionen verfügen müssen. Während IPSec-basierende VPNs auch auf Client-Seite statisch vergebene IP-Adressen erfordern, kommt das NCP-VPN auch mit der im privaten und SOHO-Bereich üblichen dynamischen Adressvergabe zurecht.

NCP ist nach eigenen Angaben bislang der einzige Anbieter, der eine Komplett-VPN-Lösung für Remote-Access-Szenarien anbieten kann. Es gibt verschiedene Versionen des VPN-Clients sowohl als Software-Lösung (verfügbar für Windows 9x, NT und OS/2) wie auch als VPN-Gateway für kleine Netze. Auf Seiten der Zentrale kommen entweder dedizierte VPN-Gateways oder eine im Network-Access-Server von NCP integrierte VPN-Lösung zum Einsatz. Beide Lösungen basieren betriebssystemseitig auf NT 4. Als PKI-(Public Key Infrastructure) ist eine Komponente des amerikanischen Herstellers Celo Communications integriert. (fbi)

NCP-Implementierung der Security-Verhandlungen in das PPP-Protokoll

NCP Engineering
Tel.: 0911/99 68-0
www.ncp.de



Hohe Verfügbarkeit für E-Business

Auf der CeBIT 2000 zeigte IBM, wie komplette Speicherlösungen für Storage Area Networks (SANs) aussehen können. Im Mittelpunkt des Geschehens stand dabei der IBM-Enterprise-Storage-Server (Codename Shark), der über die IBM-Server-Plattformen hinaus auch Nicht-IBM-Server innerhalb eines SANs integrieren kann. Durch das neuartige Feature PAV (Parallel Access Volumes) können nämlich unterschiedliche Hosts auf dasselbe Volume gleichzeitig zugreifen. Als Grundanforderung für eine hohe Verfügbarkeit ist es gelungen, ein so genanntes „Serverless Backup" zu gewährleisten. Durch die Split-Mirror-Lösung können während eines Backup-Prozesses gleichzeitig Datenbank-Transaktionen durchgeführt werden.



IBMs neue SAN-Test-Center bietet die Möglichkeit, heterogene SAN-Lösungen zu evaluieren

In Sachen Tape zeigte das neue IBM-3590-E-Bandsystem, welche Performance Bandspeichermedien heute für Backup und Recovery bereitstellen. Das gesamte SAN-Szenario kann dabei im laufenden Betrieb über die Web-basierte Storwatch-Managementkonsole konfiguriert und verwaltet werden. IBM präsentierte außerdem im Rahmen einer Demo die Einbindung von LTO-(Linear-Tape-Open-)Bandsystemen als Zusatz zu NAS- und SAN-Lösungen.

IBMs neues SAN-Test-Center in Mainz stellt auf rund 4000 Quadratmetern das Wissen und die Erfahrung von über 300 Speicherexperten von IBM zur Verfügung. Es bietet Kunden die Möglichkeit, heterogene SAN-Lösungen mit Komponenten unterschiedlichster Hersteller auf Interoperabilität, Zuverlässigkeit, Skalierbarkeit und Sicherheit zu evaluieren. Das Angebot reicht von Performancemanagementtests, Applikationstests in SAN-Umgebungen, Backup- und Recovery-Tests bis zum umfassenden Consulting über alle Phasen der SAN-Implementierung. Neben Funktionen der Storage-Manager-Software für das Netfinity-Fibre-Channel-Storage-Subsystem stellt IBM fünf neue SAN-Managementapplikationen führender Software-Hersteller vor, die auf der IBM-Netfinity-Server-Linie basieren. (kl)

IBM
Tel.: 0 18 03/31 32 33
www.ibm.com

Modem mit ADSL-Zugriff

Zur CeBIT 2000 präsentierte Eicon Technology das erste Produkt der DIVA-ADSL-Familie, die DIVA ADSL+V.90. Das Modem ermöglicht den Zugriff auf unternehmensinterne Netze, schnellen Internet-Zugang und Fax-Server-Funktionalität via ADSL mit einer Übertragungsgeschwindigkeit von bis zu 1,5 Mbps. Darüber hinaus unterstützt die Karte den V.90-Standard und bietet damit auch einen schnellen Analogzugang von bis zu 56 kbps. Die DIVA ADSL+V.90 gewährleistet dem Nutzer, über eine einzige Telefonleitung gleichzeitig zu telefonieren oder ein Fax zu senden und im Web zu surfen. Das Produkt soll ab Juli 2000 verfügbar sein.

Die Karte bietet einen hilfreichen Setup-Wizard für Anwender der Betriebssysteme Windows 98 und Windows 2000, womit sich die Karte in drei Schritten einrichten lässt. Das Modem integriert ein automatisches Diagnose-Tool, das bei Bedarf Auskunft über den gegenwärtigen Zustand der Karte gibt. Falls ein Problem auftritt, liefert es dem Nutzer sofort selbstständig die nötigen Informationen zur Fehlerbehebung. (kl)



Die DIVA ADSL+V.90 ermöglicht eine Übertragungsgeschwindigkeit von bis zu 1,5 Mbps

Eicon Technology Diehl
Tel.: 01 80/5 59 9111
www.eicon.de



DMS für kleinere Firmen

Mit „Docuware Business for Excellent“ stellte Docunet zur CeBIT eine Schnittstelle zu den betriebswirtschaftlichen Lösungen der Exact-Gruppe vor. Das Interface erlaubt die schnelle Integration des Dokumentmanagement-Systems (DMS) „Docuware Business“, eines speziell auf den Bedarf mittelständischer Unternehmen zugeschnittenen Lösungspakets, mit der Produktlinie „Excellent“. Excellent bildet die Nachfolge-Software für die verschiedenen Systeme der in der niederländischen Exact-Gruppe zusammengeschlossenen Software-Häuser, in Deutschland unter anderem Exact Szymaniak Software (mit Bavaria Soft), PCAS und DB-Soft.

Die Migration zu einer Produktlinie, die über moderne Funktionalität beispielsweise für Customer-Relationship-Management und E-Business verfügt, erhält durch die einfache Anbindung an Docuware eine weitere wichtige Option. Mit Docuware stehen komfortable Funktionen für Dokumentmanagement und elektronische Archivierung zur Verfügung, die ohne großen Einführungsaufwand produktiv eingesetzt werden können. Für den Einsatz in kleinen und mittleren Unternehmen ist die Produktversion Docuware Business geeignet, die – bei gewissen Einschränkungen gegenüber dem Funktionsspektrum des Hauptprodukts Docuware 4.1 – die Systemadministration weiter vereinfacht. Ein späteres Upgrade auf Docuware 4.1 lässt sich ohne großen Aufwand durchführen. (kl)



Docuware Business vereinfacht die Systemadministration und lässt sich ohne großen Aufwand auf Docuware 4.1 upgraden

Docunet
Tel.: 089/89 44 33 0
www.docunet.de

SAN-Lösungen für das E-Business

Auf der CeBIT 2000 präsentierte Hitachi Data Systems mit Open-Systems-Data-Center eine skalierbare offene SAN-Lösungen, die auf der Hitachi-Freedom-Data-Networks-(FDN-)Architektur aufbaut. Die konventionelle Internet-Konfiguration, basierend auf einer 100-Megabit-Technologie, wird damit um das Sechsfache übertroffen. Im Data Center wurde die Open-Systems-Funktionalität vorgeführt, die durch die Interoperabilität von Industriestandard-SAN-Komponenten und der Hitachi-Freedom-Storage-5800-Produktfamilie erreicht wird. Hitachi Data Systems und seine Allianzpartner stellen vier Schlüsselkomponenten für SAN bereit: Speichersysteme wie beispielsweise Hitachi Data Systems Freedom Storage, Verbindungselemente wie Router, Hubs und Switches; Host-Bus-Adapter und zentrale Management Software. (kl)

Hitachi Data Systems
Tel.: 00 44-17 53/61 85 50
www.hitachi-eu.com

Universeller Web-Client für Archivsystem

Win!DMS stellte auf der CeBIT einen neuen Web-Client für sein Dokumentenmanagement- und Archivierungssystem Saperion vor. Der Client basiert auf ActiveX und hat nach Herstellerangaben keinerlei Einschränkungen gegenüber der nativen Windows-Version. Zu den unterstützten Funktionen gehören zum Beispiel Capturing, Dokumentenmanagement, Dokumenten-Workflow, Archivierung und Jukebox-Management. Einzige Voraussetzung ist die lokale Installation der passenden Scanner-Treiber. Alle Datenbankzugriffe werden über das von Win!DMS selbst entwickelte virtuelle RPC-Protokoll über das Web an einen Gateway-Server versendet, der dann die Aufgaben stellvertretend für den Client ausführt und die Ergebnisse an den Web-Client kommuniziert.

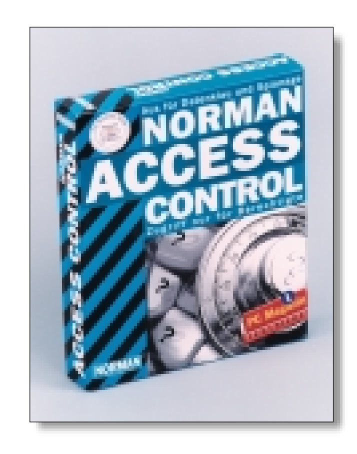
Weitere in Hannover vorgestellte Neuerungen betrafen eine Schnittstelle zu Lotus Notes, die in Zusammenarbeit mit dem Notes-Systemhaus Kasten Consulting entwickelt wurde sowie die Integration in Novells NDS als weitere Plattform neben Windows NT. Die Active-Directory- und LDAP-Integration befinden sich derzeit noch in Entwicklung. (fbi)

Win!DMS
Tel.: 030/6 00 60-204
www.saperion.de

Absicherung großer Netzwerke

Die Zugriffs- und Verschlüsselungs-Software Norman Access Control verhindert einen unerlaubten Zugriff auf Daten und Systemfunktionen von PCs und Laptops. Die auf der CeBIT neu vorgestellte „Creeping encryption“-Funktion beschleunigt die Verschlüsselung um ein Vielfaches. Sie verschlüsselt nur die tatsächlich genutzten Bereiche der Festplatte. Mit dem neuen Norman Access Control 5.0 können E-Mails und E-Mail-Attachments direkt aus MS Outlook einfach und schnell versandt werden. Das erweiterte Desktop-Management ermöglicht eine zentrale Verwaltung aller Zugriffsrechte.

Öffentlich zugängliche PCs können mit dem Kiosk Mode sicher genutzt werden. Unbekannte Benutzer haben nur auf ganz bestimmte Funktionen Zugriff. Moderne Chipkartentechnik, variable Passwortregeln oder biometrische Systeme klären die Identität des jeweiligen Anwenders. In Verbindung mit dem Norman-Security-Server erleichtert Norman Access Control 5.0 das zentrale Management von Chipkartenbenutzern. Hier wurde die Unterstützung von Smart Cards mit eingebautem Kryptoprozessor weiter verbessert. (kl)



Bei Norman Access Control lassen sich mit einem Mausklick alle Systemeinstellungen sicher administrieren

Norman Data Defense Systems
Tel.: 0212/2 6718-0
www.norman.de



Virtuelle Disk mit bis zu 20 Terabyte

Auf ihren CeBIT-Ständen präsentierte Grau Data Storage die innovative Network-Attached-Speicherlösung (NAS) „Infinistore Virtualdisk (IVD)" sowie deren Integration in verschiedene Systemumgebungen für die Datensicherung und Datenarchivierung aus Dokumentenmanagement, SAP R/3, Audio- und Videosystemen. Mit dem Replizierungsmodul von Grau Data Storage können die Daten im Virtualdisk-System redundant in dasselbe System oder in ein Zweitsystem geschrieben werden. Das optionale Modul der Infinistore-Systemlösung unterstützt sowohl den Unicode-Zeichensatz als auch Verzeichnistrukturen mit mehr als 256 Zeichen. Darüber hinaus werden alle NT-spezifischen Dateizugriffsrechte identisch übergeben.

Das IVD-System integriert in einem kompakten Gehäuse Magnetbandroboter, Bandlaufwerke, Medien, einen Windows-NT-Server, RAID-5-Festplattenspeicher und die Infinistore-Virtualdisk-Software für das Speichermanagement. Als Network Attached Storage Device stellt sich die Speicherlösung nach außen als logisches Festplattenlaufwerk dar und ermöglicht damit eine Plug-and-play-Integration in beliebige Netzwerkumgebungen. Die Architektur der IVD basiert auf einem zweistufigen Speicherprinzip mit einem RAID-5-Festplattensystem und der Migration der Daten nach HSM-Regeln auf Bandmedien. Für anspruchsvolle Anwendungen lässt sich das – auf bis zu 20 Terabyte erweiterbare – System auch mit Fibre Channel-, ATM- oder Gigabit-Ethernet-Anbindung konfigurieren. (kl)



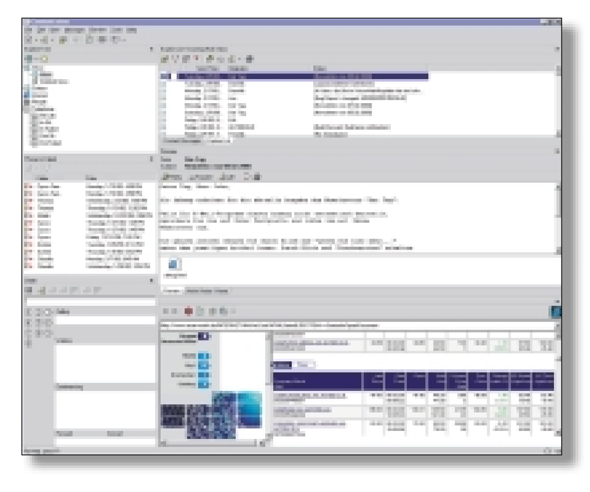
Die Administration des IVD von Grau ist von jedem Rechner im LAN aus über ein Java-basierendes Tools möglich

Grau Data Storage
Tel.: 07171/187-212
www.graudatastorage.de

Unified Messaging per Web und WAP

Für den Bereich Advanced Unified Messaging hat Cycos zur CeBIT die Version 3.50 von Mrs der Öffentlichkeit vorgestellt. Das Produkt soll das Spektrum von Advanced Unified Messaging um zwei weitere Funktionalitäten ergänzen. Mit Mrs 3.50 kann der Anwender nicht nur Fax, E-Mail, Voice-Mail, SMS und CTI flexibel über den Bildschirm nutzen, sondern ihm werden auch noch zusätzliche Zugangswege über Web und WAP ermöglicht – alles über einen Server. Mrs 3.50 ist einfach bedienbar und leicht zu integrieren in die Umgebungen Microsoft Exchange, Lotus Notes und SAP R/3.

Für den Internet-Zugang zur Mailbox ist keinerlei zusätzliche Software nötig. Durch die Unterstützung des WAP-Protokolls können Nachrichten sogar über das Handy gelesen werden. Weiter ist es möglich, auf diese Weise Voice-Mail-Meldungen abzuspielen und Rückrufe zu initiieren. Mrs 3.50 bietet neben den Unified-Messaging-Funktionen Fax, E-Mail und SMS zusätzlich auch die Integration von Computer-Telefonie (CTI). Damit lassen sich über die PC-Tastatur alle Funktionen eines Komforttelefons nutzen. Für den Systemadministrator bleibt der Verwaltungsaufwand gering: Das System kann über Exchange administriert werden, die Replikation aktueller Daten erfolgt automatisch.



Mit Mrs 3.50 von Cycos kann der Anwender zusätzliche Zugangswege über Web und WAP nutzen

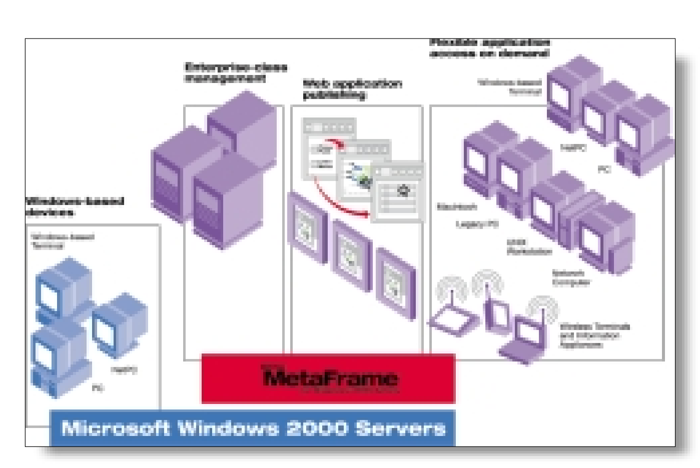
Cycos
Tel.: 02404/901129
www.cycos.com



Application-Server für Windows 2000

Auf der CeBIT hat Citrix Systems eine aktuelle Version ihres Produkts „Metaframe“ angekündigt. Metaframe 1.8 für Microsoft-Windows-2000-Server ergänzt die Windows-2000-Plattform um die zentralen Funktionen, mit denen sich Metaframe in den vergangenen Jahren als Lösung für Application-Server-Computing unter Windows NT 4.0 etabliert hat. Die neue Version von Metaframe macht Windows 2000 auch Endgeräten zugänglich, die nicht auf Windows basieren. Sie ist außerdem das erste Produkt der Metaframe-Produktfamilie, in das die neu entwickelte Web-Portal-Technologie Citrix Nfuse integriert ist. Mit Nfuse können Applikationen von einer Citrix-Metaframe-Server-Farm aus auf Web-Seiten verteilt werden. Der Zugriff auf die Applikationen erfolgt dann über einen Web-Browser. Citrix Nfuse stellt eine schnelle und einfache Möglichkeit dar, Applikationen Web-fähig zu machen.

Die dynamischen Load-Balancing-Services von Metaframe sorgen dafür, dass der Anwender zu dem am wenigsten ausgelasteten Server geleitet wird, um so eine optimale Ressourcen-Nutzung zu gewährleisten. Die Secure-ICA-Services sichern die Netzwerkdaten durch eine End-to-End-Verschlüsselung des ICA-Datenstroms. Mit Hilfe der Installation-Management-Services können Administratoren Software innerhalb einer Citrix-Server-Farm von einer zentralen Stelle aus replizieren. (kl)



Mit Metaframe 1.8 für Microsoft-Windows-2000-Server kann man auf 32-Bit-Anwendungen mit beliebigen Geräten zugreifen

Citrix Systems
Tel.: 0811/83 00 00
www.citrix.de

Neu im deutschen Server-Markt

Der Bereich Computersysteme von Toshiba erweitert sein Produktportfolio um eine neue Familie von PC-Servern. Zusammen mit den zunächst vier Server-Systemen präsentierte sich Toshiba auf der CeBIT mit einer umfassenden Palette an Computersystemen: von Notebooks über Desktop PCs und Mini-Tower-Modelle bis hin zu Servern. Die steigende Nachfrage nach Komplettlösungen aus einer Hand ist unter anderem durch die stark wachsende Bedeutung von flexiblen, ortsungebundenen PC-Arbeitsplätzen bedingt. Dies verlangt nach einem veränderten Aufbau von IT-Infrastrukturen in Unternehmen. Gefordert sind mobile End-to-End-Netzwerke, die hohen Sicherheitsstandards genügen, leicht zu verwalten sind und kostengünstige mobile Konnektivität ermöglichen. Toshiba entschloss sich daher – durch die im Bereich mobile Computing gesammelte Erfahrung – jetzt auch für den Remote Access optimierte Server-Systeme anzubieten. Die in Regensburg hergestellten vier Magnia-Modelle (Magnia 500D, 3030, 5100, 7010) richten sich an unterschiedliche Zielgruppen, wobei sich Toshiba sowohl auf große als auch auf kleine und mittlere Unternehmen fokussiert. (kl)

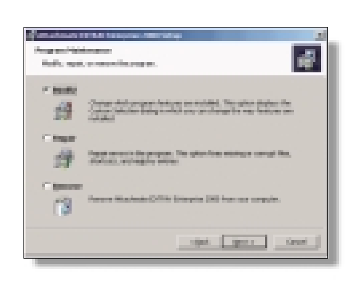


Der Magnia 5100 von Toshiba wird mit modernen Management-Tools ausgeliefert

Toshiba Computersysteme
Tel.: 018 05/22 42 40
www.toshiba.de/computer

Host-Connectivity für Windows 2000

Das auf der CeBIT neu vorgestellte Produkt „Extra! Enterprise 2000“ von Attachmate ergänzt die umfassende Connectivity-Familie des Unternehmens. Es erfüllt die Zertifizierungsanforderungen für Windows 2000 Professional und unterstützt die erweiterten Funktionen des neuen Betriebssystems. Der so genannte Roaming-Profile-Support ermöglicht es den Anwendern, von jedem PC in einem Netzwerk aus auf ihre eigenen, individuell konfigurierten Connectivity-Applikationen zuzugreifen. Extra! Enterprise 2000 nutzt die neue Windows-Installer-Technik, die selbsttätig fehlerhafte Installationen korrigiert und ohne Bediener selbstständig durchführt. Die verbesserten Power-Management-Funktionen von Windows 2000 und Extra! Enterprise stellen sicher, dass Host-Verbindungen auch im Sleep-Modus aufrecht erhalten werden.



Extra! Enterprise 2000 unterstützt auch die Self-Repair-Funktionen von Windows 2000

Das Connectivity-Produkt unterstützt proprietäre und Standard-Connectivity-Optionen für Mainframe- und Multihost-Umgebungen. Neben dem erweiterten Connectivity-Komfort erfüllt die neue Lösung mit der Secure Socket Layer-(SSL-)Verschlüsselung hohe Sicherheitsstandards beim Datentransfer. Extra! Enterprise 2000 ist kompatibel zu den Microsoft-Terminal-Services.

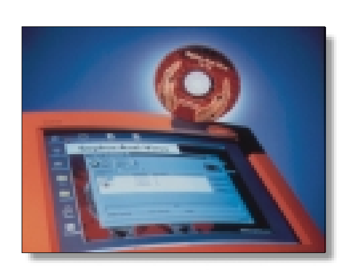
Damit sind Windows 2000 und die neuesten Anwendungen auch per Emulation zugänglich, unter Verwendung der vorhandenen PCs. (kl)

Attachmate
Tel.: 089/9 93 51-203
www.attachmate.de



Virenfrei unter Windows 2000

Die auf der CeBIT vorgestellte Software „Sophos Anti-Virus (SAV)“ hat die ICSA Zertifizierung für das Aufspüren von Viren unter Windows 2000 erhalten hat. Die ICSA setzt für kommerzielle Sicherheitsprodukte die Standards und liefert dafür unabhängige und objektive branchenübergreifende Programme zur Produktzertifizierung. Um die ICSA-Anti-Viruszertifizierung unter dem Windows-2000-Betriebssystem zu erhalten, müssen Produkte 100 Prozent aller in der Öffentlichkeit gefundenen Viren per On-Demand- und On-Access-Scan aufspüren. Die Software ist auf Exchange- oder Domino-Servern installiert und bietet drei verschiedene Betriebsarten: Sie kann jede Zieldatei jeweils auf Anfrage nach Viren untersuchen (On-Demand), diese Dateien zu festgelegten Tagen und Uhrzeiten prüfen (Scheduled) oder auch empfangene oder zu verschickende E-Mail-Anhänge abfangen und untersuchen (Real-time). Eine umfassende Protokollisierung informiert Administratoren, Absender und Adressaten über etwaige Viren. (kl)



SAV findet Viren auch in Anhängen, die mit ZIP oder anderen populären Werkzeugen komprimiert worden sind

Sophos
Tel.: 0 61 36/9119-3



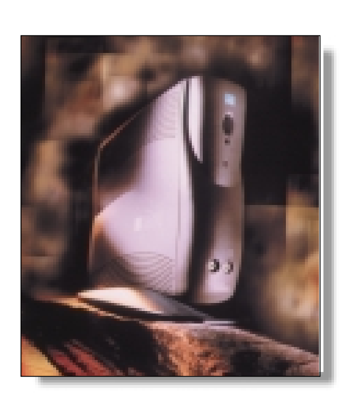
Lotus erweitert Client-Portfolio für Web-Browser und Palmtops

Im Mittelpunkt der Lotus-Präsentation auf der CeBIT standen die neuen Clients für den Zugriff auf den Groupware- und Messaging-Server Domino, die bereits zuvor auf der Lotusphere in Orlando erstmals der Öffentlichkeit vorgestellt wurden. Neben dem nativen Notes-Client will Lotus unter dem Namen iNotes in Zukunft auch einen mit reichhaltigen Funktionen ausgestatteten Web-Client anbieten. iNotes enthält die Lotus-Domino-Offline-Services, mit denen Domino-Anwendungen auch im Offline-Modus verfügbar werden. Web-Clients können somit ebenso wie bereits seit langem die nativen Notes-Clients auch ohne Netzwerkverbindung Daten bearbeiten, die später mit dem Server abgeglichen werden. Die zweite wichtige Neuerung für den Web-Client ist iNotes Access für Microsoft Outlook. Damit erhalten Outlook-Anwender Zugriff auf die Messaging- und Calendaring-Funktionen des Domino-Servers. Mit dem ebenfalls vorgestellten Lotus Mobile Notes sollen schließlich auch Anwender mit Handhelds, Palmtops und intelligenten Telefonen auf Notes-Anwendungen zugreifen können. Die Funktionalität soll dabei erheblich über das bereits heute verfügbar Intellisync hinausgehen.

Als weiteres Highlight präsentierte Lotus einen Technologie-Preview auf sein kommendes Knowledge-Management-Portal „Raven". Als integrierte KM-Suite umfasst Raven ein „Enterprise Knowledge Portal" mit Funktionen zur Erstellung und Verwaltung von Profilen über Benutzer und Interessengemeinschaften sowie eine so genannte „Discovery-Engine". Letztere besteht wiederum aus dem „Expertise Locator", der demografische und Interessensprofile verwaltet sowie dem „Content Catalog". Raven ist nicht auf Domino-Umgebungen festgelegt und wird als eigenständiger Server installiert. Es benutzt unter anderem Code von Domino R5, DB2, Lotus Sametime, InXight und Keyview. Als Clients wird – zumindest für die Version 1 – der Internet Explorer 5 vorausgesetzt. Die Beta von Raven wird noch für dieses Frühjahr erwartet. Die ersten Kunden sollen Mitte des Jahres das fertige Produkt erhalten. (fbi)

Lotus Development
Tel.: 01 80/5 41 23
www.lotus.de

Thin Clients unter Windows 2000



Die Thinstar-400-Familie ermöglicht die Host-Einbindung in Firmensysteme

Auf der CeBIT 2000 stellte NCD ihre neue Thinstar-400-Produktfamilie vor. Der auf Windows CE basierende Thinstar 400 hat als CPU einen Intel-166-MHz-Pentium-Prozessor. Ausgerüstet mit 16 MB Flash Memory kann das System bis auf 288 MByte Hauptspeicher hochgerüstet werden. Durch seine Vielseitigkeit kann die Thinstar-400-Familie unter Windows NT (Terminal Server Edition) oder Windows 2000 eingesetzt werden und ermöglicht zudem einen einfachen Web-Zugang und Host-Einbindung in Firmensysteme, aber das bei einfachster Instandhaltung und Verwaltung. Der NCD Thinstar 450 ist für den Einsatz als Microsoft Windows-based Terminal Professional (WBT Pro) konzipiert, das auf NT 4.0 Workstation aufbaut. Unterstützt werden dadurch Embedded Internet Explorer 5.0 mit Zugang zu Windows Applikationen über RDP und/oder ICA.

Anfang des Jahres hatte NCD den Entwickler von Server-Software Multiplicity bekanntgegeben. Diese Erweiterung des NCD Portfolios brachte eine strategische Leistungsanalyse und Kapazitätsplanung für Windows NT Netzwerke und Windows 2000 Server. Das Unternehmen wird ein Multiprotokoll Verwaltungswerkzeug liefern, um zeitkritische Lösungen über Multiserver-Plattformen wie Microsoft-Terminal-Services anzubieten. Die Software eignet sich für große Server-Installationen und verteilte Netze. (kl)

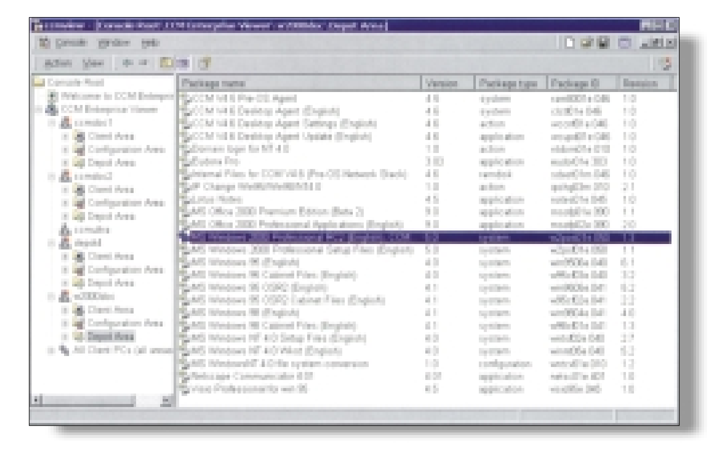
Network Computing Devices
Tel.: 089/4 58 72 80
www.ncd.de

Beschleunigte Migration

Die auf der CeBIT von On Technology vorgestellte Software On Command CCM für Windows 2000 beschleunigt die Migration von Windows 2000 Professional durch eine automatisierte Installation von Betriebssystem und Applikationen von einer Reihe von Server-Plattformen aus – einschließlich Windows 2000, Windows NT 4.0 und Unix. Die Implementierung des Active Directory in die jeweilige Umgebung kann dabei erst später vorgenommen werden.

Der „Scheduled-Push"-Ansatz von On Command CCM reduziert Netzwerk- und Server-Loading durch interaktionsfreie Ferninstallation über Nacht oder am Wochenende. Dies ergänzt den „Software-on Demand" Enduser-Pull-Ansatz, der von Microsoft beim Gebrauch von Windows 2000 und Intellimirror bereitgestellt wird. (kl)

On Technology
Tel.: 0 81 51/36 90
www.on.com



On Command CCM ermöglicht IT-Administratoren die Verwaltung heterogener Client-Umgebungen



Thin-Clients auf Geode-Basis



Das schnurlose Geode WebPAD dient zum Surfen im Internet sowie für den Zugriff auf E-Mail-Dienste

Zur CeBIT demonstrierte National Semiconductor eine Reihe fortschrittlicher Thin-Client-Lösungen. Gemeinsam mit National zeigte IBM das Windows-basierte Terminal (WBT) „Network Station“, das auf der National-Geode-Prozessortechnologie basiert. Das WBT von IBM dient für den Zugriff auf Applikationen unter Windows 2000 oder Windows NT 4.0. Die in dem neuesten Thin-Client von IBM zum Einsatz kommende Lösung enthält den Prozessor des Typs National Geode GXLV-233, ergänzt durch I/O-, Audio-Codec-, Spannungsregler- und verschiedene andere Peripherie- und Analogchips. Herzstück der Lösung ist der Geode GXLV von National. Dieser mit integrierten Grafik-, Audio- und Speichersteuerungsfunktionen sowie einem PCI-Interface ausgestattete Prozessor stellt einfach anzuwendende Multimedia-Technologie zur Verfügung, die sich für Thin-Client-Umgebungen eignet. (kl)

National Semiconductor
Tel.: 0 81 41/35 12 84
www.national.com

Aktives Kundenmanagement

Auf der CeBIT 2000 führte die CAS Software ihr Kundeninformationssystem Genesisworld in der Version 2.0 vor. Eine neue Schlüsselfunktionalität ist die Historienüberwachung für Vertriebsleiter, Key-Account-Betreuer und Projektleiter.

Darüber hinaus bietet Genesisworld 2.0 eine Datenreplikation für Niederlassungen und Notebooks sowie eine Anbindung an Microsoft Outlook. Das Unternehmen stellte zudem Freeoffice vor, den neuen, kostenlosen Internet-Dienst für Genesisworld-Anwender und Privatpersonen. Freeoffice bietet einen umfangreichen Kalender, ein Adressverzeichnis und eine zugriffsgeschützte Dokumentenverwaltung. Im Bereich der geografischen Business-Anwendungen zeigten CAS Software und PTV die neue Einstiegslösung Map&Guide Reference, Erweiterungen der professionellen Routenplanung Map&Guide 6 sowie neue Versionen des geografischen Planungssystems Map& Market und des Flottenmanagementsystems Map&Guide Fleet Monitor. (kl)

CAS Software
Tel. 0721/9638-188
www.cas.de

Permanent verfügbare Hochleistungs-Server

Stratus Computer, Anbieter der nach eigenen Angaben weltweit zuverlässigsten Server, kündigt eine neue Serie fehlertoleranter Server für geschäftsrelevante Anwendungen und E-Commerce-Lösungen auf Grundlage von Windows 2000 auf der CeBIT an. Stratus und Microsoft arbeiteten bei Software-Design und -Engineering zusammen, um die hohe Verfügbarkeit des neuen Betriebssystems noch zu steigern. Stratus plant die offizielle Vorstellung der Server-Linie auf Windows-2000-Basis, einem neuen Hardware-Design, umfangreichen Software-Verfügbarkeits-Features und Rund-um-die-Uhr-Service für April 2000.

Stratus ergänzt das Betriebssystem Windows 2000 durch seine fehlertolerante Technologie, ohne den Kernel anzutasten. Der Kunde soll die Anwendungen „out of the box“ auf den neuen Servern starten könne. Gemeinsam wollen Microsoft und Stratus einen nahtlosen Rund-um-die-Uhr-Kundenservice für Hardware und Betriebssystem anbieten. (kl)

Stratus Systems
Tel.: 0 61 96/47 25-0
www.stratus.com

Innovative Drucklösungen

Den Schwerpunkt ihres Messeauftritts legte Lexmark in diesem Jahr auf die Präsentation von Drucklösungen. Mit AHT Image Manager können bei einem Anschaffungspreis von unter 100.000 Mark bis zu 210 Seiten/Minute gedruckt werden. Die Clustering-Lösung von AHT verteilt einen Druckauftrag auf bis zu sechs Drucker und macht so die zügige Verarbeitung von Massendruck möglich, sorgt für Flexibilität und ständige Verfügbarkeit. Mit der Reporting-Software „Marktrack“ können die gesamten Druckkosten erfasst und beispielsweise den jeweiligen Abteilungen zugeordnet werden. Außerdem informiert die Software unter anderem über die Auslastung der jeweiligen Drucker im Unternehmen. Die Druckermanagement-Software „Markvision“ überwacht und administriert alle Drucker innerhalb eines Netzwerks und ermöglicht zum Beispiel zentralisiertes Setup und Konfiguration von Netzwerkdruckern oder auch Fernbedienung und Druckermanagement in Echtzeit.



Lexmarks Drucklösungen sind kompatibel zu allen Lexmark-Monochrom- und -Farb-Laserdruckern der neuen Generation

Mit „Optra Forms“ lösen elektronisch gespeicherte Formulare vorgedruckte Formularsätze ab. Die ebenfalls auf der Messe gezeigte Lexmark-Drucklösungen für SAP ermöglichen professionelles Drucken aus R/3. So erlauben die speziellen Druckertreiber für R/3 beispielsweise die Ansteuerung aller Papieroptionen. (kl)

Lexmark
Tel.: 08 00/5 39 62 75
www.lexmark.de

ISDN-Anwendungspakete für NT und Windows 2000

		ISDN-Kommunikationsfunktionen des angebotenen ISDN-Anwendungspakets																			Software unterstützt				Anwendungsschnittstellen					Sonderfunktionen					ISDN- und Kommunikationsschnittstellen		
Anbieter Telefon	Produktname (Hersteller)	Telefax Gruppe 3	Telefax Gruppe 4	Telex/Teletex	Euro-Filetransfer	Terminal-Emulation	T-Online-Zugang	File-Transfer	Fax on Demand	E-Mail-Messaging	Telefonie	Anrufbeantworter	Voice-Box	Remote LAN-Access	zentraler Internet-Zugang	Remote Control	virtuelle CAPI am Arbeitsplatz	TK-Anlagen-Funktionalität	weitere ISDN-spezifische Telematikfunktionen	weitere nicht ISDN-spezifische Telematikfunktionen	max. Zahl der B-Kanäle	Kanalbündelung	Datenkompression	Verschlüsselung	MS-Exchange	Lotus Notes	Novell Groupwise	Integration in E-Mail/Groupware	sonstige	univ. Message-Box	einheitl. Adressbuch	Client-Zugriff über Web-Browser	Programmierfähigkeit	eigener Client	CAPI 1.1	CAPI 2.0	sonstige
Acotec 46706-77	Remote Access Manager 21 for NT RAS									●				●		●					120	●	●	●				●	SNMP, RAS			●		●		●	SNMP
AVM 030/39976-242	ISDN Multi Protocol Router																		LAN-LAN-Kopplung via ISDN IBSM OS2	SSM, HDSL-Anbindung	120	●	●	●												●	PPPOE
	ISDN Access Server													●						GSM-Remote Access	120	●	●	●					NT-Benutzer-DB, Radius-Server			●	●	●		●	
	NDI																●				120								NT-Benutzerverwaltung			●		●	●		
	AVM Ken!	●			●	●		●	●	●	●	●			●		●				2	●	●									●		●		●	
	AVM Ken! DSL	●			●	●		●	●	●	●	●			●		●			ADSL	2	●	●									●		●		●	
CA Computer Ass. 089/62724-0	Faxserve	●								●											32				●		●	●		●				●		●	
CAE Elektronik 02402/106-300	Caesar	●	●	●				●	●	●		●	●						CTI, Unified Messaging	SMS, WAP	14				●	●	●	●	SAP R/3, R/2	●	●	●	●	●		●	
Cisco Systems 01803/671001	Cisco 700, 800, 2600		●				●	●	●	●	●	●		●	●	●	●	●				●	●	●	●	●	●	●		●	●	●	●	●		●	
Com:On 040/23658-300	C3-Web	●	●	●	●				●	●	●	●	●						GSM/SMS, Document on Demand		bel.				●	●	●	●	Standard Webbrowser	●	●	●	●	●		●	
	C3-Messenger	●	●	●	●				●	●	●	●	●						dto.		bel.				●	●	●	●		●	●		●	●			
	C3-Faxx	●			●														dto.		bel.				●	●	●	●		●	●			●		●	
	C3-Fax	●			●																bel.				●	●	●	●		●	●			●		●	
Consultix 0421/33388-0	Faxwave Telex Connector			●															Wap opt.		30		●		●		●	●	Interchange Connect	●	●	●	●	●		●	
	Faxwave Universal	●	●	●				●	●	●		●	●						Wap opt.		30		●		●		●	●	dto.	●	●	●	●	●		●	Faxclass 2/2.0
	Faxwave Fax Connector	●	●						●	●									Wap opt.		30		●		●			●	Interchange Connect	●	●	●	●	●		●	Faxclass 2/2.0

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

ISDN-Anwendungspakete für NT und Windows 2000

Anbieter Telefon	Produktname (Hersteller)	ISDN-Kommunikationsfunktionen des angebotenen ISDN-Anwendungspakets																			Software unterstützt				Anwendungsschnittstellen					Sonderfunktionen					ISDN- und Kommunikationsschnittstellen		
		Telefax Gruppe 3	Telefax Gruppe 4	Telex/Teletex	Euro-Filetransfer	Terminal-Emulation	T-Online-Zugang	File-Transfer	Fax on Demand	E-Mail-Messaging	Telefonie	Anrufbeantworter	Voice-Box	Remote LAN-Access	zentraler Internet-Zugang	Remote Control	virtuelle CAPI am Arbeitsplatz	TK-Anlagen-Funktionalität	weitere ISDN-spezifische Telematikfunktionen	weitere nicht ISDN-spezifische Telematikfunktionen	max. Zahl der B-Kanäle	Kanalbündelung	Datenkompression	Verschlüsselung	MS-Exchange	Lotus Notes	Novell Groupwise	Integration in E-Mail/Groupware	sonstige	univ. Message-Box	einheitl. Adressbuch	Client-Zugriff über Web-Browser	Programmierfähigkeit	eigener Client	CAPI 1.1	CAPI 2.0	sonstige
	Faxwave Voice Connector											●	●								30		●		●			●	Interchange Connect	●	●	●	●	●		●	
Copia International 030/723922-49	Fax Facts Copia International								●		●														●									●			
CSG 0251/23004-0	Aupos	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			bel.	●	●	●		●		●	MS-Outlook	●	●	●	●	●	●	●	
	Boxsoft	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			bel.	●	●	●		●		●	MS-Outlook	●	●	●	●	●	●	●	
DCT Dolphin 06227/605-605	Call XPress 5.3 (AVT)	●	●	●							●	●	●		●			●					●		●	●				●	●	●	●				
	Faxination 4.0 (Fenestrae)	●	●	●					●											SMS			●		●				SMTP/Pop 3	●	●					●	
	Rightfax 7.0 (Rightfax)	●							●	●											60		●		●	●	●	●	SMTP/Pop 3	●	●	●	●	●			
Derdack 0331/29878-0	Message-Master Corp.									●						●			SMS, Paging, WAP						●	●		●		●	●	●	●	●			
Digi International 0231/9747-630	Datafire Micro V/3.0/ Pico	●			●				●		●	●	●			●					2	●	●								●					●	
Equisys 0044/20/7203-4000	Zetafax	●																			60				●	●	●	●		●	●		●	●		●	
Faxscape Europe 0231/97575-130	Faxscape 2000	●							●								●					●			●			●		●	●	●	●	●		●	
IA Information Systems 0941/5855660	Continuum	●	●			●			●	●	●	●	●	●	●	●		●				●	●	●	●	●		●		●	●	●				●	
INW 040/639188-24	Tobit-David (Tobit)																																				
	Fax Serve CA	●						●													32					●		●								●	

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

LAB-Report Marktübersicht

ISDN-Anwendungspakete für NT und Windows 2000

ISDN-Kommunikationsfunktionen des angebotenen ISDN-Anwendungspakets

Anbieter Telefon	Produktname (Hersteller)	Telefax Gruppe 3	Telefax Gruppe 4	Telex/Teletex	Euro-Filetransfer	Terminal-Emulation	T-Online-Zugang	File-Transfer	Fax on Demand	E-Mail-Messaging	Telefonie	Anrufbeantworter	Voice-Box	Remote LAN-Access	zentraler Internet-Zugang	Remote Control	virtuelle CAPI am Arbeitsplatz	TK-Anlagen-Funktionalität	weitere ISDN-spezifische Telematikfunktionen	weitere nicht ISDN-spezifische Telematikfunktionen
Isoft 030/723922-0	Catway						●													
	Cat						●													
	Mobile Manager						●		●				●	●						
	Webbill																			
Infin 089/745152-0	Fax Facts + Voice Facts	●							●	●	●	●	●	●	●	●		●		
Janus HST 040/897181-0	V Capi 4.0 (HST)				●			●									●			
	DVS 2.0 (HST)				●			●								●				
	Remote Server (HST)																			
Kamell Software 0661/96730	The Box										●	●	●			●	●			
Krauss Systeme 0511/319274	David 6 Pro.	●							●	●		●	●			●		●	DDI	
	GFIFax (GFI)	●																		
Lansource 05206/4124-0	Faxport für Exchange V 7.0	●																	ISDN-Routing	
	Faxport für Lotus Notes V 7.0	●																	ISDN-Routing	
	Faxport für NT V.7.0	●																	ISDN-Routing	
	Winport Dial Out V.7.0																●		virtuelle Com-Ports	Com-Port-Sharing

Software unterstützt / Anwendungsschnittstellen / Sonderfunktionen / ISDN- und Kommunikationsschnittstellen

Anbieter Telefon	Produktname (Hersteller)	max. Zahl der B-Kanäle	Kanalbündelung	Datenkompression	Verschlüsselung	MS-Exchange	Lotus Notes	Novell Groupwise	Integration in E-Mail/Groupware	sonstige	univ. Message-Box	einheitl. Adressbuch	Client-Zugriff über Web-Browser	Programmierfähigkeit	eigener Client	CAPI 1.1	CAPI 2.0	sonstige
Isoft 030/723922-0	Catway	bel.	●		●						●		●	●				IP
	Cat	bel.	●		●								●		●			IP
	Mobile Manager			●		●	●		●						●		●	TAPI
	Webbill				●								●					
Infin 089/745152-0	Fax Facts + Voice Facts	180				●					●	●		●	●			
Janus HST 040/897181-0	V Capi 4.0 (HST)	30	●													●	●	
	DVS 2.0 (HST)	30	●	●	●							●		●		●	●	
	Remote Server (HST)											●						
Kamell Software 0661/96730	The Box	30													●		●	
Krauss Systeme 0511/319274	David 6 Pro.	250				●	●		●	SMTP	●	●	●	●	●	●	●	
	GFIFax (GFI)	50				●	●		●	SMTP	●	●			●		●	
Lansource 05206/4124-0	Faxport für Exchange V 7.0	bel.				●					●	●		●			●	
	Faxport für Lotus Notes V 7.0	bel.					●				●	●		●			●	
	Faxport für NT V.7.0	bel.										●	●	●	●		●	
	Winport Dial Out V.7.0	bel.	●	●	●												●	

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

ISDN-Anwendungspakete für NT und Windows 2000

Anbieter Telefon	Produktname (Hersteller)	ISDN-Kommunikationsfunktionen des angebotenen ISDN-Anwendungspakets																			Software unterstützt				Anwendungsschnittstellen					Sonderfunktionen					ISDN- und Kommunikationsschnittstellen		
		Telefax Gruppe 3	Telefax Gruppe 4	Telex/Teletex	Euro-Filetransfer	Terminal-Emulation	T-Online-Zugang	File-Transfer	Fax on Demand	E-Mail-Messaging	Telefonie	Anrufbeantworter	Voice-Box	Remote LAN-Access	zentraler Internet-Zugang	Remote Control	virtuelle CAPI am Arbeitsplatz	TK-Anlagen-Funktionalität	weitere ISDN-spezifische Telematikfunktionen	weitere nicht ISDN-spezifische Telematikfunktionen	max. Zahl der B-Kanäle	Kanalbündelung	Datenkompression	Verschlüsselung	MS-Exchange	Lotus Notes	Novell Groupwise	Integration in E-Mail/Groupware	sonstige	univ. Message-Box	einheitl. Adressbuch	Client-Zugriff über Web-Browser	Programmierfähigkeit	eigener Client	CAPI 1.1	CAPI 2.0	sonstige
Lightning Instr. 0041/21/6542000	Multicom-Backup IV							●		●				●	●	●			Clug, Sub, CLI	IP, IPX, Bridge, NAT, PAT, Firewall	8	●	●	●	●	●	●	●				●		●			
	Pocket Multicom							●		●				●	●	●			Clug, Sub, CLI	dto.	2	●	●	●	●	●	●	●				●		●			
	Multicom LAN Access Center							●		●				●	●	●			Clug, Sub, CLI	IP, IPX, Bridge, NAT, PAT, Firewall	60	●	●	●	●	●	●	●				●		●			
Maier 0711/3060-0	MRS (Cycos)	●	●	●	●			●	●	●	●	●	●								60				●	●	●					●		●		●	
Materna 0231/5599-00	Office Editory	●			●				●	●	●	●	●				●	●							●	●				●	●	●		●	●	●	
NCP 0911/9968-0	RWS/GA	●			●		●	●		●	●	●		●		●					8	●	●	●									●		●	●	
Network Domains 08021/8879-0	Courga (Callware)										●	●	●					●				●			●	●	●	●		●	●	●	●	●			
	Callegra (Callware)										●	●	●						Sprache wie E-Mail	intell. Telefon-Beantworter		●			●	●	●	●		●	●	●	●	●			
	Messagelan-Faxgate/ Lanfax (Esker)	●								●										für alle gängigen TKs		●			●	●		●		●	●	●	●	●			
Option International 0032/16/317411	GSM-Ready 56K/ISDN PC Card Mode	●				●		●		●							●				2	●	●		●							●				●	
Ositron 0241/94698-42	Ositron VMS	●	●	●	●		●	●	●	●	●	●	●	●	●		●				50	●		●	●					●	●	●	●	●		●	
Ritz Soft-Media 089/74016993	Voice Connect	●			●			●	●	●	●	●	●		●	●		●			96	●	●	●	●			●		●		●				●	
RTE Software 0033/1/45744500	RTE Fax für Microsoft Exchange	●																			256	●			●					●	●	●	●	●		●	
	RTE Fax für Lotus Notes/Domino	●								●											256	●				●				●	●	●	●	●		●	

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

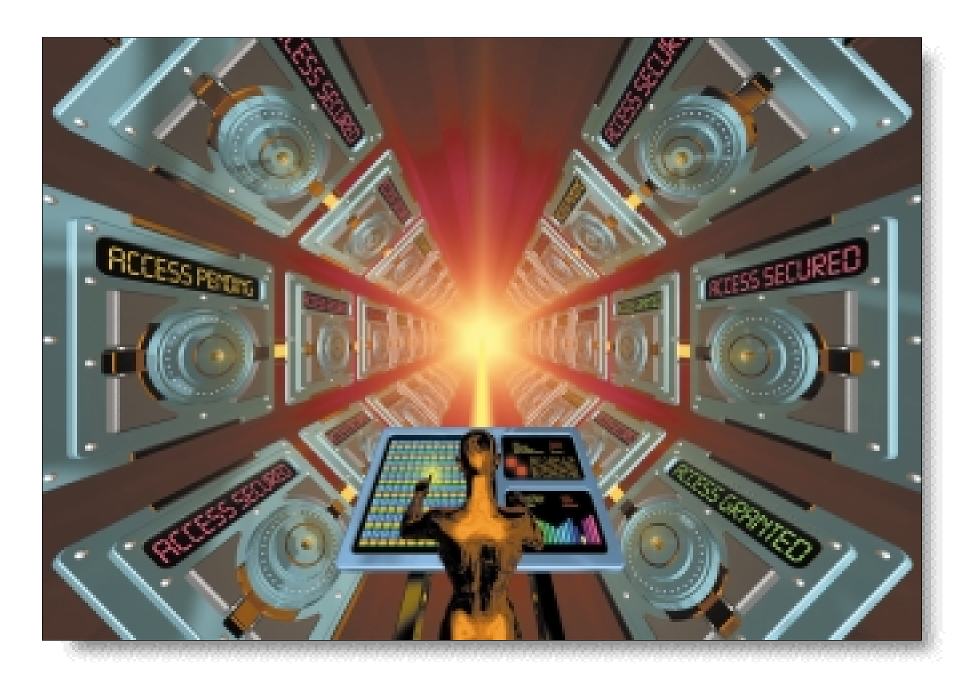
ISDN-Anwendungspakete für NT und Windows 2000

Anbieter Telefon	Produktname (Hersteller)	ISDN-Kommunikationsfunktionen des angebotenen ISDN-Anwendungspakets																			Software unterstützt				Anwendungsschnittstellen					Sonderfunktionen					ISDN- und Kommunikationsschnittstellen		
		Telefax Gruppe 3	Telefax Gruppe 4	Telex/Teletex	Euro-Filetransfer	Terminal-Emulation	T-Online-Zugang	File-Transfer	Fax on Demand	E-Mail-Messaging	Telefonie	Anrufbeantworter	Voice-Box	Remote LAN-Access	zentraler Internet-Zugang	Remote Control	virtuelle CAPI am Arbeitsplatz	TK-Anlagen-Funktionalität	weitere ISDN-spezifische Telematikfunktionen	weitere nicht ISDN-spezifische Telematikfunktionen	max. Zahl der B-Kanäle	Kanalbündelung	Datenkompression	Verschlüsselung	MS-Exchange	Lotus Notes	Novell Groupwise	Integration in E-Mail/Groupware	sonstige	univ. Message-Box	einheitl. Adressbuch	Client-Zugriff über Web-Browser	Programmierfähigkeit	eigener Client	CAPI 1.1	CAPI 2.0	sonstige
RVS Datentechnik 089/35498-0	RVS-Com Professional 1.6	●	●		●	●	●	●			●	●	●		●	●							●		●											●	
S. Punkt 0241/1829334	Sprech.Way Call Center	●	●							●	●	●	●					●			2-8												●			●	
Secunet 06196/95888-0	Sicherheitsberatung	●	●	●	●		●	●		●	●	●	●	●	●	●		●			bel.	●	●	●													
Servonic 08142/47990	Ixi Server	●							●	●	●	●	●			●		●	SMS		30		●		●	●		●	SAP R/1, SMTP-Messaging	●	●	●	●			●	
SK-Computerdienst 0211/36975-34	k. A.				●	●	●	●		●	●			●		●									●											●	
Teles 030/3992800	Teles RVR-Power Pack	●	●		●	●		●	●		●	●									2	●	●		●			●		●						●	
Thetakom 06157/9153-17	MRS (Cycos/Thetakom)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	SMTP, ACD, SMS, VDO	Web, WAP, Archiv	bel.				●	●	●	●	Baan, SAP	●	●	●	●	●		●	
Tobit Software 02561/9130	David Professional	●							●	●	●	●	●					●	Fax Plus		250				●	●	●	●	DIIE	●	●	●	●	●		●	
Topcall 0711/727240	Communication Server One	●		●					●	●		●	●		●						128				●	●	●	●	SAP, AS/400, Netscape, Host	●	●	●	●	●			
Trend Communications 089/323009-36	Aurora																	●	ISDN Handtestgeräte		30								MS-Win, Win NT								
Valuesoft 089/99120-0	Gateland, Isline, Twinfax	●			●	●	●	●	●		●	●	●	●	●		●	●	RAS		60	●	●	●	●	●	●	●	SAP-R/3		●		●	●		●	
Haus Weilgut 07243/5466-0	Weilgut Contact								●	●	●															●											

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

Anwendungen mit Windows Terminal Server und Citrix Metaframe sicher im Internet publizieren

Thin Clients auf sichere Art



von David Carroll

Immer mehr Firmen nutzen das weltumspannende Netz als technische Infrastruktur, um Kunden, Lieferanten und Mitarbeiter an die eigene EDV anzubinden. Eine besonders komfortable und flexible Möglichkeit bietet die Publikation von Windows-Anwendungen über den Windows NT Terminal Server und Citrix Metaframe. Doch jede Anwendung, die nach außen geöffnet wird, stellt auch ein Sicherheitsrisiko dar. Wir sagen Ihnen, wie Sie den Konflikt zwischen Offenheit und Sicherheit lösen können.

Anwendungen über das Internet zu publizieren, liegt im Trend. Den so genannten Application Service Providern (ASPs) wird von vielen Analysten eine glorreiche Zukunft vorausgesagt. Schließlich ersparen sie dem Anwender teure Investitionen in eigene Hardware, Software und Infrastruktur. Auch zur Anbindung von Kunden, Lieferanten und externen Mitarbeitern ist das Internet als Anwendungs-Infrastruktur attraktiv.

Allerdings sind geschäftskritische Anwendungen, die komplett über einen Web-Browser bedient werden können, noch Mangelware. Was liegt näher, als mit Hilfe des Microsoft Terminal Servers bestehende Windows-Anwendungen über das Internet zu verbreiten. Besonders komfortabel wird dies mit dem Zusatzprogramm Citrix Metaframe, das die Anwendungen auf beinahe jeder Client-Maschine verfügbar machen kann, sei es Windows, OS/2 oder auch Linux. Schon heute setzen viele Firmen die Kombination von Windows NT Server 4.0 Terminal Server Edition (WTS) und Citrix Metaframe ein, um ihre auf Windows basierenden Anwendungen einer breiten Benutzerbasis zur Verfügung zu stellen.

Diese Möglichkeit besteht dank Citrix ICA. ICA ist ein Industriestandard zur Bereitstellung von Firmenanwendungen für eine große Palette von Desktop-Plattformen und Netzwerkprotokollen. Mit ICA kann der Server die Anwendungslogik von der Benutzerschnittstelle trennen und nur die grafische Oberfläche der Anwendung an den Client senden. Die Anwendung wird vollständig auf dem Server ausgeführt. Anwendungen, die mit Hilfe von ICA an Clients verteilt werden, benötigen zum Teil nur ein Zehntel der Netzwerkbandbreite, die sie normalerweise beanspruchen, d.h. ungefähr 10 bis 20 KB pro Benutzersitzung.

Beim Einsatz einer ICA-basierten Thin-Client-Lösung ist neben der Performance-Optimierung und der genauen Anwendungskonfiguration vor allem der Sicherheitsaspekt zu beachten. Schließlich sollen die veröffentlichten Anwendungen den richtigen Personen problemlos zugänglich sein, ohne dabei Sicherheitslöcher in das Netzwerk zu reißen.

Man muss wissen, wie Anwendungen außerhalb einer Firewall zur Verfügung gestellt werden können, aber auch wie dabei eine hohe Sicherheitsstufe gewährleistet werden kann. Es macht

wohl jeden Netzwerkadministrator nervös, wenn Ports an einer Firewall geöffnet werden. Zur Wahrung der Netzwerksicherheit müssen Sie die Verfahren kennen, wie ICA-Sitzungen durch verschiedene Arten von Firewalls an den Client gesendet werden, und Sie müssen wissen, wie die Firewall und die ICA-Einstellungen zur Minimierung des Risikos konfiguriert werden können.

Dynamische Ports Das ICA-Protokoll von Citrix ist ein proprietäres Netzwerkprotokoll, das über TCP/IP betrieben wird. Wie das FTP-Protokoll arbeitet ICA mit dynamischer Port-Zuordnung, um einem Client das Erreichen des Servers über das Internet zu ermöglichen. Ein Client kann eine Sitzung mit ICA auf zwei Arten beginnen: Entweder, er stellt eine direkte Verbindung zum Server her und empfängt einen vollständigen fernen NT-Desktop, oder er durchsucht die Server nach der Anwendung, falls der Administrator die Anwendungen veröffentlicht hat.

Im Falle einer direkten Server-Verbindung findet die einleitende Synchronisierung zwischen dem Client und dem Server über TCP-Port 1494 statt. Der Rest der Sitzung erfolgt dann allerdings über einen dynamisch zugeordneten Port. Wenn der Benutzer nach einer veröffentlichten Anwendung sucht, erfolgt die einleitende Synchronisierung über UDP-Port 1604. Der Server gibt über einen dynamischen Port die IP-Adresse eines Servers zurück, der eine Liste der verfügbaren Anwendungen enthält. Dann richtet der Client eine Verbindung zu der Anwendung über TCP-Port 1494 ein, und der Rest der Kommunikation läuft wiederum über einen dynamischen Port.

Dieses Verfahren kann bei Firewalls, die zum Schutz des Server- oder Client-Netzwerks installiert sind, recht knifflig werden. Die meisten Firewalls können mit ICA nichts anfangen. Daher kann es geradezu eine Herausforderung sein, eine Konfiguration herzustellen, in der eine Firewall das ICA-Protokoll passieren lässt. Die meisten jedoch nicht alle Firewalls können dennoch so konfiguriert werden, dass sie das ICA-Protokoll passieren lassen.

Der Hauptsuchdienst ohne Firewall Der Server, der für die Verfolgung verfügbarer ICA-Funktionen (z.B. verfügbarer Citrix-Server, verfügbare veröffentlichte Anwendungen, Lizenz-Pools, Leistungs- und Auslastungsinformationen für Citrix-Server) zuständig ist, wird als Hauptsuchdienst (Master Browser) bezeichnet. Der Suchdienst-Server funktioniert ähnlich wie der Suchdienst (Browser Service) von Microsoft. Auf jedem Citrix-Server ist der ICA-Suchdienst aktiv und erwählt einen Citrix-Server zu seinem Hauptsuchdienst. Alle anderen Citrix-Server im Netzwerk sind Mitgliedssuchdienste (Member Browsers). Jedes physische Netzwerk von Citrix-Servern besitzt einen Hauptsuchdienst pro Protokoll. Der Hauptsuchdienst für jedes Netzwerk wird durch einen Wahlprozess bestimmt. Wenn der aktuelle Hauptsuchdienst in einem Netzwerk ausfällt, findet die Wahl eines neuen Hauptsuchdienstes statt, wodurch eine hohe Zuverlässigkeit des ICA-Suchdienstes erreicht wird. Jedes Transportprotokoll (z.B. TCP/IP, IPX, NetBIOS) besitzt einen Hauptsuchdienst.

Zum Empfang der Adresse eines Servers oder einer veröffentlichten Anwendung müssen Citrix-ICA-Clients den Hauptsuchdienst lokalisieren oder eine direkte Verbindung zu dem entsprechenden Server über die IP-Adresse oder die MAC-Adresse des Servers herstellen. Der Citrix-ICA-Client lokalisiert den Hauptsuchdienst, indem er Broadcast-Pakete aussendet.

Um in einem Netzwerk ohne Firewall eine Anforderung für den ICA-Suchdienst zu schicken, sendet der Client ein Paket mit der Zieladresse von UDP-Port 1604 als Broadcast an das Netzwerk. Der kontaktierte Server gibt die IP-Adresse des Hauptsuchdienstes an den Client über einen Port oberhalb von 1023 zurück. Der Algorithmus zur TCP-Port-Zuordnung indiziert alle verfügbaren Ports zwischen 1023 und 65534 und speichert einen Zähler, der den zuletzt zugeordneten Port angibt. Der Zähler wird nach jeder Zuordnung erhöht, und der Server stellt durch eine Überprüfung sicher, dass keine andere Verbindung diesen Port verwendet. Wenn eine andere Verbindung den Port verwendet, überprüft der Server den nächsten verfügbaren Port. Die TCP/IP-Port-Zuordnung ist eine Funktion der Anzahl von Verbindungen, die der Server unterhält, und kein zufälliger Prozess. Der verfügbare Benutzer-Port mit der höchsten Nummer ist standardmäßig Port 5000, jedoch kann der Registrierungsteilschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\MaxUserPort hinzugefügt und dieser Wert auf eine Dezimalziffer zwischen 5000 und dem TCP/IP-Maximum von Port 65534 gesetzt werden.

Wenn die Kommunikation erfolgreich hergestellt wird, gibt der Hauptsuchdienst eine Suchliste zurück. Zum Starten einer Anwendung wählt der Client einen Server bzw. eine veröffentlichte Anwendung aus der Suchliste aus. Alternativ dazu kann der Client eine ICA-Datei auswählen, bei der es sich um eine vorkonfigurierte Datei handelt, die für eine Anwendung spezifische Browser- und Anwendungsinformationen enthält. Die Anwendungsverbindung

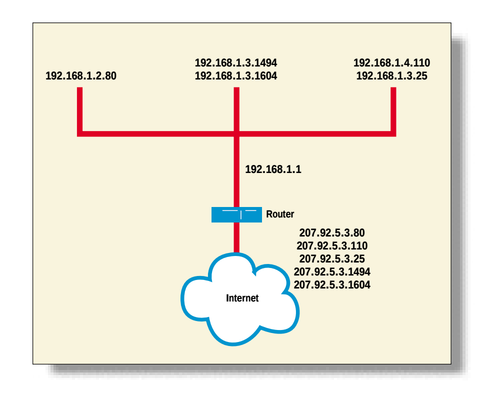


Bild 1. *Network Address Translation (NAT)*

wird über TCP-Port 1494 eingeleitet, und der Server reagiert unter Verwendung der gleichen Port-Zuordnungsmethode über einen TCP-Port mit einer hohen Nummer über 1023. Zur Erstellung einer ICA-Datei kann der Benutzer den ICA-Desktop-Editor verwenden.

Sie können auch mit dem Published Application Manager, dem Tool zur Verwaltung veröffentlichter Anwendungen, arbeiten. Wenn Sie diesen verwenden, können Sie mit einem Klick mit der rechten Maustaste auf die Anwendungen auf einen Assistenten zugreifen, der bei der Erstellung einer ICA-Datei behilflich ist. Listing 1 zeigt eine ICA-Basisdatei, in der der Eintrag „TcpBrowserAddress“ die externe IP-Adresse und der Eintrag „Desktop“ den Namen der veröffentlichten Anwendung angibt.

Firewall-Konfiguration Jeder geöffnete Port ist ein Tor, durch das sich ein Angreifer möglicherweise Zugang verschaffen kann. Eine Firewall versucht, solche Tore zu schützen. Zur Veranschaulichung ließe sich das Beispiel von Torwächtern anführen, die überprüfen, ob eine Person eintreten darf. Wenn eine Firewall hinzugefügt wird, muss diese so konfiguriert werden, dass ICA-Browser-Pakete über UDP-Port 1604 und TCP-Port 1494 durchgelassen werden. Um das Citrix-Netzwerk nach Ser-

vern und veröffentlichten Anwendungen durchsuchen zu können, muss der Client in der Lage sein, durch Port 1604 in das Netzwerk des Servers hineinzukommen und über einen beliebigen Port mit einer Nummer über 1023 wieder aus dem Netzwerk herauszugelangen. Allerdings kann auch eine direkte Verbindung zum vollen Desktop eines bestimmten Servers mit Hilfe der entsprechenden TCP/IP-Adresse über Port 1494 hergestellt werden, sodass Port 1604 nicht geöffnet werden muss.

ICA ist ein recht neues Protokoll, sodass der Einsatz einer Firewall eine ziemliche Herausforderung darstellt. Die entsprechende Firewall muss so konfiguriert werden, dass sie eine Client-Sitzung über die ICA-Ports zulässt. Die anzuwendende Konfigurationsmethode muss auf die spezifische Architektur der Firewall abgestimmt werden. Es gibt vier Hauptmodelle für die Architektur von Firewalls: Paketfilter-Gateways, Gateways auf Schaltungsebene (Circuit Relay), Firewalls mit Statusinspektion (Stateful Inspection) und Proxy-Server. (Siehe auch den Artikel von Christian Uwe Götz über die Auswahl der richtigen Firewall auf Seite 79).

Paketfilter-Gateway Paketfilter-Gateway ist die Architektur mit der einfachsten Konfiguration, aber sie bietet auch den geringsten Schutz. Zur Konfiguration eines Paketfilter-Gateways muss einfach eine Regel eingefügt werden, die einem Client erlaubt, ein eingehendes Signal an den Server über TCP-Port 1494 und UDP-Port 1604 zu senden und die eine Antwort über Port 1023 oder einen Port mit höherer Nummer zulässt. Die Methode, mit der diese Regel definiert wird, hängt von der verwendeten Firewall ab.

Gateway auf Schaltungsebene Gateways auf Schaltungsebene (Circuit-Level Gateway) implementieren eine höhere Sicherheit, da sie auf Sitzungsebene operieren und logische Verbindungen erstellen, die NT nur eine gewisse Zeitdauer beibehält. Wenn eine Client-Sitzung die Schaltung herstellt, überprüft die Firewall, ob die Sitzung die Sitzungsverbindung herstellen muss und ermöglicht dem Client dann, alle nachfolgenden Daten ohne Überprüfung zu senden. Gateways auf Schaltungsebene werden ähnlich wie Paketfilter-Gateways konfiguriert.

Firewall mit Statusinspektion Die Statusinspektion (Stateful Inspection) erweitert die Paketfilterung, indem sie Statusinformationen nach Maßgabe früherer Kommunikationsdaten und anderer Anwendungen hinzufügt. Firewalls mit Statusinspektion können wie Paketfilter-Gateways so konfiguriert werden, dass neue Protokolle durch die Firewall über bestimmte Ports hindurchgelassen werden. Darüber hinaus bietet die Statusinspektion aufgrund der beim Durchgang der Pakete durch die Firewall durchgeführten Paketinspektion eine bessere Sicherheit. Die Konfiguration des ICA-Protokolls setzt voraus, dass das ICA-Protokoll als Netzwerkdienst konfiguriert wird.

Proxy-Server In der Regel dienen Proxies zur Überwachung des abgehenden Verkehrs. Einige Anwendungs-Proxies speichern angeforderte Daten in einem Cache und protokollieren Verbindungsinformationen, wodurch sich der Bandbreitenbedarf verringert, die Zugriffszeiten auf ähnliche Verbindungspunkte verkürzen und Nachweise zu übertragenen Daten erstellt werden. Es gibt zwei Typen von Proxy-Servern: Anwendungs-Proxies und SOCKS-Proxies.

Anwendungs-Proxies sind extrem sicher. Für jede Anwendung und jedes Protokoll muss eine spezielle Proxy-Regel definiert werden. Diese Proxy-Server führen eine Analyse auf Anwendungsebene durch, indem sie jedes Paket beim Passieren des Gateways untersuchen. Das Anwendungs-Proxy-Verfahren lässt sich an einer Person illustrieren, die mit FTP eine Verbindung zu einem anderen Computer herstellt. Die Person verwendet FTP, um die Verbindung zum Proxy-Server und dann von dort aus zur Außenwelt herzustellen. Ein Anwendungs-Proxy-Server automatisiert diesen Prozess.

Da Proxy-Server die komplette Kommunikation verarbeiten, können sie alle Aktionen eines Clients protokollieren. Zum Beispiel kann ein HTTP-Proxy alle URL-Adressen aufzeichnen, die vom Benutzer besucht wurden. Ein FTP-Proxy kann alle Dateien anzeigen, die heruntergeladen wurden. Diese Proxies sind in der Lage, unerwünschte Wörter, Sites und Dateien von besuchten Sites herauszufiltern, und sie können nach Viren suchen. Anwendungs-Proxies können sogar eine Authentifizierung von Benutzern durchführen, bevor sie eine Verbindung zur Außenwelt zulassen. Für einen Web-Benutzer erscheint jede Web-Site so, als würde sie eine eigene Anmeldung verlangen. Der Administrator hätte vollständige Kontrolle darüber, wie Benutzer die Verbindung nach außen nutzen. Damit ein neues Protokoll wie ICA durch einen Proxy-Server hindurchgelassen wird, muss eine spezielle Lösung für den Durchgang durch die Firewall entwickelt werden.

Ein SOCKS-Proxy-Server ähnelt einer Telefonvermittlung. Er ist gewissermaßen das Software-Gegenstück zur Schaltung von Drähten, um eine Verbindung durch das System hindurch zu einer anderen Außenverbindung herzustellen (d.h., um hinter die Firewall zu gelangen). Die meisten SOCKS-Server funktionieren nur mit TCP-Verbindungsarten.

Mit Hilfe des SOCKS-Dienstes kann ein neues Protokoll durch einen Proxy-Server hindurchgelassen werden. Es sind zahlreiche Drittherstellerprodukte verfügbar, die den Zugriff auf ICA-Anwendungen über einen Proxy-Server anbieten (z.B. Aventail Connect 3.01, Hummingbird SOCKS, NEC SocksCap32). Educational Technology hat kürzlich das Produkt Surrogate Socket entwickelt, ein Plug-in für Microsoft Proxy Server, das den Proxy-Server mit einer Möglichkeit zur Unterstützung von ICA- und RDP-Verbindungen (ohne Aktivierung des IP-Forwarding) ausstattet. Die Software für fernen Zugriff von Sun-Netscape Alliance ermöglicht es einem Unternehmen, Benutzer zu authentifizieren und ihnen einen definierten Zugriff auf Unternehmensanwendungen und -daten zu erteilen. Autorisierte Benutzer können auf vordefinierte Anwendungen über einen Java-fähigen Web-Browser zugreifen.

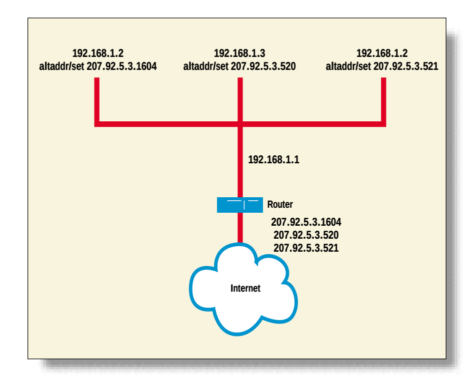


Bild 2. *Transparente statische Ports*

Auch Citrix hat angekündigt, dass sie eine Stärkung der Sicherheit des ICA-Protokolls durch eine Unterstützung von SOCKS 4.0 und 5.0 ins Auge fassen. Bei der Installation des neuesten Release-Kandidaten von MetaFrame für Windows 2000 wird der Benutzer feststellen, dass der Assistent bei der Einrichtung einer Client-Sitzung auf dem neu-

en Client fragt, ob SOCKS zur Verbindung durch eine Firewall verwendet werden soll.

Adressakrobatik Das durch das Öffnen eines Ports eingegangene Sicherheitsrisiko kann durch die Verwendung von Network Address Translation (NAT) minimiert werden. Zur Gefahrenminderung übersetzt NAT den Datenverkehr so, dass abgehender Verkehr von der Firewall zu kommen scheint und nicht vom internen Host. Im Unterschied zu Proxy-Gateways operieren NAT-Gateways innerhalb der Routing-Schicht und arbeiten technisch bedingt schneller als ihre Proxy-Gegenstücke. Das Netzwerk kann externe routing-fähige Internet-Adressen für den Router und interne nicht routing-fähige Intranet-Adressen innerhalb der Firewall verwenden. Mit Hilfe von NAT können dann die externen Adressen gemäß einer Port-Nummer in eine interne Adresse übersetzt werden. Zum Beispiel würde, wie Bild 1 zeigt, ein Client, der über NAT auf einen Server hinter dem Router zugreifen will, zunächst auf die Adresse 207.92.5.3:80 zugreifen. Das System leitet ihn dann auf die Adresse 192.168.1.2:80 um. Durch dieses Verfahren wird verhindert, dass das Netzwerk von außen direkt durchsucht werden kann. (Weitere Informationen über NAT finden Sie in dem Artikel von Zubair Ahmad auf Seite 20.)

ICA-Datei für NAT

```
[WFClient]
Version=2
TcpBrowserAddress=207.92.5.3
UseAlternateAddress=1

[ApplicationServers]
Desktop=

[Desktop]
Address=Desktop
InitialProgram=#Desktop
DesiredHRES=640
DesiredVRES=480
DesiredColor=2
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0
```

Listing 1.

Wenn Sie mit Hilfe des Published Application Managers eine ICA-Datei erstellen, wird die private Adresse als Browser-Adresse für eine Firewall definiert, die mit NAT arbeitet. In Bild 1 wäre die Browser-Adresse beispielsweise 192.168.1.3. Dieses Verfahren eignet sich gut für interne Verbindungen. Für externe Verbindungen (zum Internet) müssen Sie die generierte ICA-Datei so bearbeiten, dass sie auf die externe IP-Adresse des Hauptsuchdienstes verweist. TcpBrowserAdress in Listing 1 verweist beispielsweise auf diesen externen Port.

Wenn mit NAT eine zusätzliche Sicherheitsschicht implementiert werden soll, muss der Client außerdem die IP-Adresse des Hauptsuchdienstes anfordern. Durch Hinzufügen der Einstellung UseAlternateAddress (mit dem Wert 1) im Abschnitt WFClient in der ICA-Datei wird der Hauptsuchdienst veranlasst, dem Client die korrekte Browser-Adresse zurückzuliefern. Ohne diese Einstellung stellt der Client zwar einen erfolgreichen Kontakt zum Server her, aber der Server sendet nicht die korrekte Adresse zurück.

Zur Registrierung einer alternativen IP-Adresse dient der Befehl Altaddr. Wenn zum Beispiel die alternative IP-Adresse 207.92.5.3 einem Server zugewiesen werden soll, müssen Sie sich am Citrix-Server anmelden und auf einer Kommandozeile folgenden Befehl eingeben:

```
altaddr /set 207.92.5.3
```

Anschließend muss die ICA-Datei bearbeitet werden, um dort auf die externe Adresse zu verweisen und die alternative IP-Adresse zu verwenden (siehe Listing 1). Mit dieser Methode müssen Sie für jede Intranet-Adresse des Citrix-Servers eine gültige externe IP-Adresse angeben.

Einige Router erlauben nicht die Verwendung mehrerer externer Adressen für denselben Port. Oder es sind nicht mehrere externe Adressen vorhanden bzw. erwünscht. Durch die Zuweisung transparenter statischer Ports wird die Notwendigkeit beseitigt, für jede interne Adresse eine externe Adresse zu besitzen. Anstatt den internen Servern eindeutige Adressen zuzuweisen, wird ihnen eine Port-Nummer mit derselben externen IP-Adresse zugewiesen. Einem der Server muss Port 1604 zugewiesen werden, sodass dieser Server zum Agenten für die Lokalisierung des Hauptsuchdienstes wird. Den anderen Servern kann jeder beliebige verfügbare Port zugewiesen werden.

Um alternative Port-Nummern zuzuweisen, müssen Sie sich zunächst am Citrix-Server anmelden, der als Browser fungieren soll. Anschließend rufen Sie eine Kommandozeile auf und verwenden die Befehle icaport und altaddr. Im Beispiel aus Bild 2 findet der Citrix-Server mit der Adresse 192.168.1.2 den Hauptsuchdienst. Geben Sie dazu ein:

```
icaport /port:1604
altaddr /set 207.92.5.3:1604
```

Anschließend melden Sie sich an einem anderen Citrix-Server an und geben beispielsweise Folgendes ein:

```
icaport /port:421
altaddr /set 207.92.5.3:421
```

Mit dieser Methode kann eine Lastverteilung für eine Anwendung durch eine Firewall implementiert werden, ohne das gesamte Netzwerk einem höheren Risiko auszusetzen. Es wird nur eine externe Adresse bereitgestellt. Alle ICA-Verbindungen verwenden diese Adresse, um eine Verbindung zur Server-Farm herzustellen. Zur Bestimmung des Servers greift der Hauptsuchdienst auf die Parameter zur Auslastungsverteilung zurück, die im Load-Balancing-Administrator unter Start, MetaFrame Tools definiert werden. Und der Client empfängt die korrekte alternative Adresse und Port-Nummer.

Keine Hilfe für Eindringlinge
Jede Verbindung zu einem externen Client stellt einen potenziellen Zugang für einen ungebetenen Gast dar. Als Administrator muss man daher vollständig verstehen, wie Thin-Client-Produkte mit der Außenwelt kommunizieren. Wenn das Produkt in eine öffentliche Umgebung eingeführt wird, muss die Gefährdung des Netzwerks begrenzt werden. Die Geschichte zeigt, dass ein Angreifer mit entsprechender Motivation in jedes System einbrechen kann. Daher sollte ihm dieser Einbruch nicht auch noch erleichtert werden. Administratoren, die verstehen, wie das ICA-Protokoll mit TCP/IP arbeitet und die stärksten verfügbaren Firewalls einrichten, können die Anfälligkeit ihres Netzwerks und die Gefährdung der Informationen in Grenzen halten und weiterhin von den Vorteilen profitieren, die Citrix für Internet-Verbindungen in einer Umgebung mit schlanken Clients bietet. (fbi)

Die Auswahl der richtigen Firewall

„Fenster zu – Türen verriegeln!“

von Christian Uwe Götz*

Die Absicherung großer Netzwerke gegen Angriffe und Hacker hat sich zu einem wichtigen Bestandteil der Aufgaben von Netzwerkadministratoren entwickelt. Fast täglich lassen sich in den Medien Horrormeldungen über Einbrüche in Computernetzwerke, Datendiebstahl und die Schilderungen von möglichen Katastrophenszenarien finden. Eine Möglichkeit, sich gegen solche Gefahren zu schützen, sind Firewalls. Doch wie muss eine solche Firewall aufgebaut sein, um allen lauernden Gefahren entgegentreten zu können?



Unter einer Firewall wird häufig eine Struktur aus verschiedenen Hard- und Software-Produkten verstanden, die externe Netzwerkverbindungen einer Organisation gegen Angriffe absichern soll. Neben der reinen Implementierung einer solchen Struktur müssen weitere Maßnahmen ergriffen werden, um ein generelles Gesamtkonzept zur Absicherung eines Netzwerks nach außen und innen realisieren zu können. Eine Firewall besteht neben geeigneter Technik immer auch aus einer Sammlung von Regeln und Anweisungen, der „Security policy“. Nur probate Technik, eine wohldurchdachte und klar formulierte Policy und die strikte Einhaltung dieser Policy gewähren den erwünschten Schutz.

Firewalls können zwar viele Sicherheitsprobleme bei der Verbindung von Netzwerken lösen, bei weitem jedoch nicht alle. In den Anfangszeiten der Firewalls wurde die Virenproblematik fast gänzlich ausgegrenzt. Heute gewinnt die Absicherung der Netzwerke gegen solche Gefahren mehr und mehr an Bedeutung. Unter dem Begriff „Content-Security“ etablieren sich zunehmend Lösungen als weitere Bausteine einer Firewall-Umgebung. Um diese Art von Schutz technisch umsetzen zu können, genügt es nicht, die übertragenen

Datenpakete nur auf Protokollebene zu untersuchen. Es ist erforderlich, die Daten auch auf Applikationsebene unter die Lupe zu nehmen.

Applikations-Gateways oder Proxies arbeiten vollständig auf Applikationsebene. Die Begriffe „Gateway“ und „Proxy“ werden hier zumeist synonym verwendet. Firewalls, die auf Proxies basieren, benutzen ein Dual-Homed-Gateway, das keine IP-Pakete weiterleitet. Auf dem Gateway laufen Proxies als spezialisierte Programme ab, die in der Lage sind, Verbindungen für ein spezielles Protokoll entgegenzunehmen, die Daten auf Applikationsebene zu verarbeiten und weiterzuleiten. Das Grundprinzip nach dem Proxies arbeiten, ist die vollständige Trennung von Verbindungen zwischen dem externen und dem internen Teil einer Firewall bzw. dem Internet und dem internen Netz. Es darf keine direkte Verbindung zwischen einem externen und einem internen System bestehen.

Das bekannteste Beispiel für solche Proxies sind WWW-Caching-Proxies. Ein solcher Proxy nimmt nur Anfragen für „Internet-Protokolle“ wie HTTP, HTTPs oder auch FTP von Clients entgegen. Da ein solcher HTTP-Proxy die Semantik der Anforderung versteht, kann er auf Applikationsebene eingreifen und die gewünschte URL ermitteln. Findet der Proxy die angefragte WWW-Seite in seinem Zwischenspeicher, werden diese zwischengespeicherten Daten an den Client übermittelt. Der Vorteil hierbei liegt darin, dass die Seite nicht erneut aus dem Internet übertragen werden muss. Das spart Zeit und Geld, da Internet-Zugänge meist eine recht begrenzte Bandbreite haben und üblicherweise die übertragene Datenmenge mit dem Internet-Service-Provider abgerechnet wird.

Ein Proxy muss aber nicht zwangsläufig nur als Caching-Proxy arbeiten. Proxies gibt es für eine Vielzahl von Anwendungen und Protokollen. So kann ein Proxy auch als SMTP-Gateway agieren. Ein solcher SMTP-Proxy würde alle SMTP-Nachrichten aus dem Internet in der Gateway-Zone zentral entgegennehmen und die Nachrichten über einen zweiten Prozess an die entsprechenden Zielsysteme im internen Netz weiterleiten. Optimalerweise wird auf einem solchen SMTP-Gateway noch ein dritter Prozess ausgeführt, der Nachrichten und Dateianhänge auf Viren hin überprüft. Die Kontrolle erfolgt zentral und bevor die Nachrichten das eigene Netzwerk erreichen.

Viele Produkte in diesem Bereich bieten aber noch weitaus mehr Möglichkeiten, die Nachrichten auf unerwünschte Inhalte zu untersuchen. So kann z.B. mittels einer lexikalischen Analyse festgestellt werden, ob in dieser Mail Begriffe auftreten, die den Rückschluss zulassen, dass es sich hier um Inhalte handelt, die nicht übertragen werden dürfen. So könnte das gehäufte Auftreten des Begriffs „Bilanz“ und „DM“ den Schluss nahe legen, dass ein Mitarbeiter die Bilanzzahlen und andere Betriebsgeheimnisse offen an Dritte weiterreicht. Proxies eignen sich somit hervorragend, um auf Applikationsebene zu untersuchen, was für Daten über eine Netzwerkverbindung übertragen werden sollen. Im folgenden Abschnitt soll deshalb dieses „Was“ näher beleuchtet werden.

Content Security Um die Frage nach dem „Was“ eindeutig zu klären, bedarf es spezialisierter Tools, die Datenströme in ihrem Gesamtzusammenhang betrachten und analysieren. Dies wird unter dem Begriff „Content-Security“ zusammengefasst. Die Abgrenzung des Begriffs „Content Security“ gegenüber „Access Security“ lässt sich an einem anschaulichen Beispiel sehr einfach erklären. Ein Autofahrer möchte mit seinem PKW die Grenze ins Ausland überqueren. Hierzu muss er wie alle anderen Fahrzeuge zwangsläufig einen Grenzübergang passieren. Sofern der Grenzübergang besetzt ist, steht dort ein Grenzbeamter in Uniform. Dieser Grenzbeamte hat die Aufgabe, zu entscheiden, ob die Fahrzeuge einreisen dürfen oder nicht. Um in dieser Frage zu einer Entscheidung zu kommen, wird der Grenzbeamte anhand bestimmter Kriterien die Identität der Autofahrer ermitteln. Je nach Einschätzung eines Fahrzeugs genügt dem Beamten ein Blick auf das Kfz-Kennzeichen oder die Kontrolle der Ausweise, um sich zu entscheiden. Er interessiert sich zunächst nur für die Identität und Herkunft der vorbeifahrenden PKWs. In einzelnen Fällen hält es der Beamte aber für ratsam, etwas genauer nachzusehen und fordert die Fahrzeuginsassen auf, den Kofferraum zu öffnen oder vielleicht das gesamte

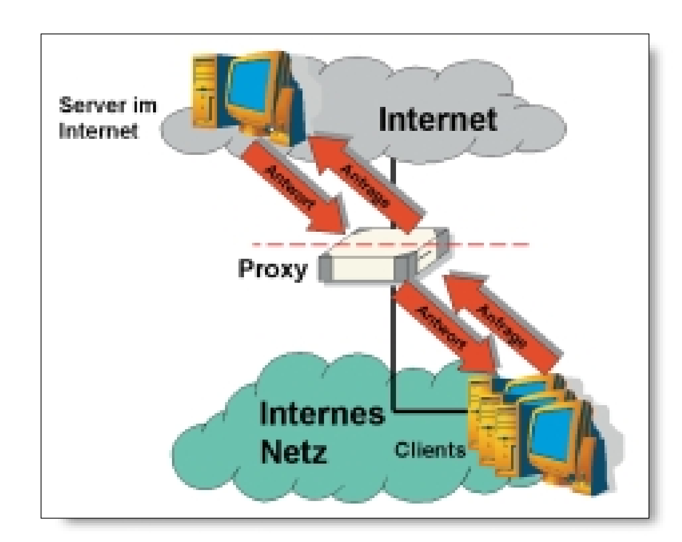


Bild 1. *Funktionsweise eines Proxies*

Fahrzeug auszuräumen. Er möchte wissen, was die Reisenden mit sich führen und ob die mitgeführten Gegenstände eventuell zu verzollen sind oder gar nicht eingeführt werden dürfen.

Übertragen auf eine Netzwerkumgebung wären die Fahrzeuge IP-Pakete und der Grenzübergang ein Gateway, eine Firewall. Der Grenzbeamte wäre zum einen für die Sicherstellung der „Access Security“ verantwortlich („Wer will passieren?“), zum anderen hat er sich für die Sicherstellung der „Content-Security“ („Was wird transportiert?“) zu interessieren.

An diesem banalen Beispiel wird deutlich, dass eine einzelne Kontrollmethode nicht allen Anforderungen zur Absicherung der Grenzen und zur Einhaltung geltender Gesetze genügen kann. Die Klärung der Frage, wer einreist, hat zunächst keine Bedeutung für die Antwort auf die Frage, was dieser Reisende mit sich führt. Ähnlich wie im Beispiel des Grenzbeamten verschwimmen die Grenzen zwischen „Access Security“ und „Content-Secuity“ zunehmend. Modernere Firewalls integrieren zunehmend Funktionen zur Sicherstellung der „Content Security“ direkt oder bieten Schnittstellen, um spezialisierte Tools nahtlos zu integrieren.

Warum Content Security? Die Methoden, mit denen Netzwerke angegriffen werden, haben sich seit den ersten Tagen der Computernetzwerke grundlegend geändert. Musste man sich früher vornehmlich gegen direkte Einbruchsversuche schützen, lauert heute eine Vielzahl von versteckten Gefahren in den Datenströmen selbst, die sich teilweise nur sehr schwer aufdecken lassen. Traditionell sind Computerviren eine der größten Gefahren, die in den Netzen kursieren. Auch hier hat sich in den letzten Jahren eine dramatische Weiterentwicklung dieser kleinen Störenfriede bemerkbar gemacht. Waren früher vornehmlich ausführbare Dateien die Träger von Computerviren, sind es heute so genannte Makroviren, die die Hersteller von Antiviren-Software immer wieder vor neue, scheinbar unlösbare Probleme stellen.

Mit der zunehmenden globalen Vernetzung hat auch die Verbreitungsgeschwindigkeit rasant zugenommen. Computerviren lassen sich durch einen einzigen Mausklick in kürzester Zeit auf mehrere 1000 Computersysteme übertragen. Oftmals bemerken die Empfänger solcher E-Mails die ungebeten Gäste gar nicht oder viel zu spät.

Als Beispiel sei hier „Melissa“ genannt, ein Virus, der in ein Microsoft-Word-Makro eingebettet war. Nach seiner Aktivierung verschickte dieser Virus wahllos an Empfänger auf der Festplatte befindliche Dokumente per E-Mail. Die Zieladressen entnahm dieses „Makro“ dem Adressbuch des auf den infizierten Rechnern installierten Mail-Clients Microsoft Outlook. Es kam zu einer wahren Mail-Flut, da Melissa an bis zu zwei Dutzend Empfänger Nachrichten mit Anhängen verschickte und sich so über diesen Weg selbst wieder weiterverbreitete.

Trojanische Pferde oder kurz Trojaner werden unbemerkt auf einem Computersystem platziert und dort aktiviert. Ein klassisches Beispiel für solch einen Trojaner ist die Übermittlung aller auf einem Computer durchgeführten Tastatureingaben an einen Empfänger außerhalb des Netzwerks, in dem sich der betreffende Computer befindet. Der Empfänger dieser Daten wird so früher oder später an Passwörter und andere sensible Daten gelangen.

Die zunehmende Ausbreitung und Nutzung des „World Wide Webs“ hat einige ganz neue Facetten von Gefahren für Netzwerke zu Tage gebracht. Sind Computerviren quasi ein Übel, das der „MS-DOS-basierten“ Computerwelt entstammt, so wurden diese Grenzen durch die Einführung von Sun Microssystems Java und Microsofts ActiveX-Technologie weitgehend gesprengt. Einer der großen Vorteile dieser Technologien ist deren Plattformunabhänigkeit. Um ActiveX-Controls und Java-Applets korrekt ausführen zu können, benötigen diese oftmals Zugriff auf die lokale Festplatte eines Computers. Unzureichend verfügbarer Hauptspeicher und begrenzte Bandbreiten zwingen zur lokalen Zwischenspeicherung solcher Codes. An dieser Stelle haben „hostile applets“ Zugriff auf lokale Ressourcen wie den Hauptspeicher oder können auf der Festplatte befindliche Daten zerstören oder manipulieren [2]. Unter einem „hostile applet“ wird Applet oder im weitesten Sinne ein Programm verstanden, das nach der Übertragung über das Netzwerk auf das Zielsystem versucht, exklusiven Zugriff auf lokale Systemressourcen zu bekommen oder versucht, diese Ressourcen in einer unerwünschten Art und Weise zu beanspruchen. Zerstört ein solches Applet Daten, wird es auch als „malicious applet“ bezeichnet [3]. Eine Demonstration eines solchen gefährlichen Applets und dessen Funktionsweise lässt sich im WWW unter http://www.security7.com/Test/Test.html finden.

Die mögliche Infizierung von Computersystemen mit solchen „hostile applets“ oder „malicious applets“ erfordert eine Neudefinition des Begriffs „Computerviren“. Unter einem Computervirus wurde bislang ein Stück Software-Code verstanden, der sich selbst durch Anhängen an eine ausführbare Datei weiterverbreitet. Um einen solchen Virus zu aktivieren, ist es üblicherweise notwendig, dass der Benutzer die infizierte ausführbare Datei startet. Im Falle der Viren in ActiveX-Controls und Java-Applets ist dies nicht mehr notwendig. Hier genügt das bloße Aufrufen und Laden einer WWW-Seite.

Eine indirekte Bedrohung ganz anderer Art ergibt sich aus den im WWW angebotenen Inhalten. In vielen Unternehmen gehört es zum Frühsport, die Bundesligatabellen zu inspizieren, Börsenkurse zu überprüfen oder andere Inhalte von WWW-Seiten zu begutachten. Nicht immer entspricht dies dem Wunsch des Managements, insbesonde-

re dann, wenn pornographische, rassistische oder gewaltverherrlichende Inhalte aus dem WWW heruntergeladen werden. Die Rechtslage ist hier derzeit in der Bundesrepublik Deutschland etwas kritisch, sodass sich die Anbieter solcher Internet-Dienste, also z.B. auch Arbeitgeber, hier absichern müssen. In einigen Fällen ist schon der bloße Besitz von verbotenen Daten (z.B. Bilder vom kinderpornographischen Darstellungen) strafbar.

Eine Methode, um diesen Auswüchsen entgegenzutreten, ist das „URL-Screening" oder „URL-Filtering". Ein Proxy überprüft jede aufgerufene URL (Universal Resource Locator). Findet sich eine URL in einer Liste bzw. Datenbanken von unerwünschten WWW-Seiten wieder, wird die Übertragung dieser Seite unterbunden. Entscheidend für die Qualität eines solchen URL-Screenings ist die zur Verfügung stehende Datenbasis mit unerwünschten URLs. Einige verfügbare Tools bieten hier die Möglichkeit, auf täglich aktualisierte Datenbanken zugreifen zu können. Neue Websites mit entsprechenden Inhalten schießen wie Pilze aus dem Boden. Das Bestreben eine solche Liste von Hand zu pflegen, dürfte wohl hoffnungslos sein. Die in den Datenbanken gesammelten URLs sind Kategorien zugeordnet, welche sich selektiv sperren oder freigeben lassen. Diese Listen lassen sich manuell erweitern, oder einzelne Seiten und Kategorien können nur zeitweise gesperrt oder zugelassen werden. So könnten z.B. die Fußballtabellen zwischen 8:00 und 12:00 Uhr und von 13:00 bis 17:30 tabu sein, während in der Mittagspause durchaus ein Blick auf dieselben erlaubt wird.

Die hier beschriebenen Rettungsversuche zur Beherrschung solcher Gefahren erscheinen mehr oder minder geglückt. Viele Administratoren neigen an dieser Stelle zur „Holzhammermethode" und verbieten die Übertragung von Java und Active-X gänzlich. Im Bereich der E-Mails werden dann schlicht keinerlei Anhänge mehr zugelassen. Allerdings stehen diese Maßnahmen oftmals den Anforderungen der Benutzer grundlegend entgegen und stören definierte Business-Prozesse. Bleibt als die Frage, wie eine schlagkräftige Firewall-Umgebung gestaltet sein sollte, damit man sich bestmöglich gegen lauernde Gefahren schützen kann?

In den vorangegangen Abschnitten wurde erwähnt, dass Proxies als Teil einer Firewall eingesetzt werden sollten. Um der Firewall-Umgebung eine Struktur zu verleihen, werden Systeme mit ähnlichen Aufgaben innerhalb der Firewall in eigenen Zwischennetzen zusammengefasst. Die Zwischennetze werden „Demilitarisierte Zonen" oder kurz DMZ genannt. So könnte es eine Proxy-DMZ geben, in der alle eingesetzten Proxies stehen. In einer weiteren DMZ könnten alle Server stehen, auf die aus dem Internet direkt zugegriffen werden kann wie z.B. der WWW-Server mit der Homepage eines Unternehmens.

Die Art und Weise, wie die einzelnen Proxies in diesem Beispiel angeordnet wurden, ist rein exemplarisch. Die Clients senden ihre HTTP-Request zum WWW-Caching-Proxy. Im optimalen Fall kann dieser Proxy die gewünschte Seite in seinem Zwischenspeicher finden und die Daten sofort an den Client zurückliefern, ohne die Daten an weitere Proxy-Stufen weiterzuleiten. Befinden sich die gewünschten Daten nicht im Proxy-Cache, wird die Anfrage über die weiteren Proxy-Stufen weitergeleitet. Ist die angeforderte URL allerdings beim URL-Filtering-Proxy als gesperrt vermerkt, bekommt der Benutzer vor dem Client nur die Meldung zu sehen, dass die gewünschte Seite nicht angezeigt werden kann. Wenn die URL nicht gesperrt ist und der zuständige WWW-Server im Internet verfügbar ist, liefert dieser die angeforderten Daten zurück. Die Daten werden auf Viren und andere gefährliche Inhalte hin überprüft und an den Client gesendet. Wichtig ist an dieser Stelle die Tatsache, dass der gesamte HTTP-Verkehr immer über Proxies abgewickelt wird. Ein Client sollte nie direkt mit einem externen WWW-Server Kontakt aufnehmen können.

Was für WWW-Daten gilt, sollte auch für E-Mails gelten. Der SMTP-Server im internen Netz liefert seine E-Mails bei einem SMTP-Gateway in der DMZ ab. Dort werden die eingehenden und ausgehenden Nachrichten auf Viren hin überprüft. Eingehende, infizierte Mails dürfen das interne Netz erst gar nicht erreichen. Dass der interne Mail-Server allerdings trotzdem noch über einen eigenen Virenscanner verfügen sollte, um verseuchte Nach-

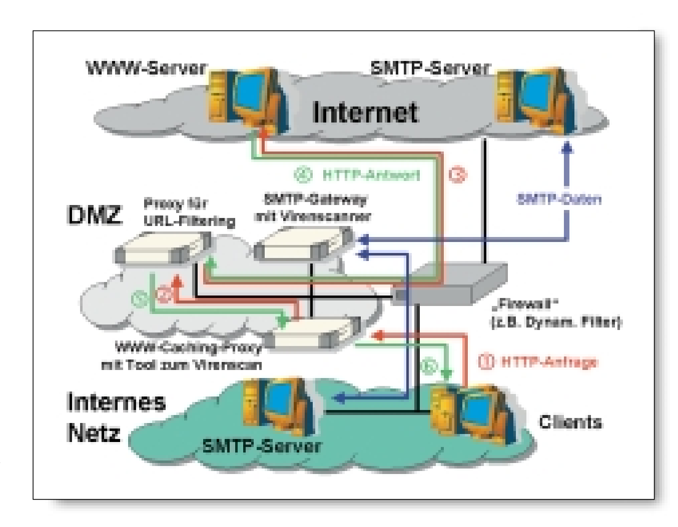


Bild 2. *Typisches Szenario für die Umsetzung von „Content Security"*

richten im eigenen Netz aus dem Verkehr zu ziehen, versteht sich von selbst.

Nicht alles was glänzt ist Gold

Nicht alle Produkte dienen zur Erkennung von Gefahren gleich gut. Oftmals ist es erforderlich, mehrere Produkte parallel einzusetzen. So kann ein Tool z.B. sehr gut in HTTP-Streams gepackte Java-Applets und ActiveX-Controls auf unerwünschte Inhalte hin untersuchen, aber es bietet keine Möglichkeit, ein URL-Screening durchzuführen oder auch FTP-Übertragungen auf Viren hin zu untersuchen.

Leider kann ein Browser immer nur mit einem Proxy direkt in Kontakt treten. Diese Adresse kann sich während einer Sitzung nicht beliebig ändern. Aus diesem Grund kommt es zwangsläufig zu einer Kettenbildung mehrerer Proxies. So müssen sich die WWW-Daten z.B. zuerst durch einen Caching-Proxy schlängeln und werden dann von diesem an einen HTTP-Proxy übergeben, der Applets auf gefährliche Inhalte hin untersucht. Dieser wiederum gibt die geprüften Daten an einen Proxy weiter, der ein URL-Screening durchführt. So entsteht unversehens eine Kette von mehreren Proxy-Stufen. Jede Stufe erfordert Rechenleistung und Zeit, unabhängig davon, ob nun eine der Stufen stark belastet ist oder nicht. Diese Kettenbildung kann also zu einer spürbaren Verlangsamung der Datenübertragung zum Client hin führen.

Die Frage, wie ein solche Kette optimalerweise aussieht und welche Komponenten an welcher Stelle der Kette zu stehen haben, lässt sich nicht pauschal beantworten. Hier spielen sehr viele Parameter wie die Art des eingesetzten Produkts, verwendete Betriebssysteme und der Typ der verwendeten WWW-Browser eine Rolle. Viele Probleme beim Aufbau solcher Proxychains lassen sich aber auf eine unglücklich gewählte Reihenfolge der eingesetzten Komponenten zurückführen.

Der Markt der Virenscanner ist heute fast unüberschaubar. Jeder Hersteller rühmt sich mit noch höheren Erkennungsraten und noch schnelleren Scan-Engines. Ein guter Virenscanner zeichnet sich jedoch nicht einzig und allein dadurch aus, wie schnell er ist und wie viele verschiedene bekannte Viren er erkennt. Ebenso wichtig sind Antworten auf die Fragen, wie gut der Scanner ineinandergeschachtelte Files auseinanderdividieren kann und wie tief diese Verschachtelung sein darf, damit sie der Scanner noch entflechten kann oder wie schnell Updates für den Scanner erhältlich sind. Was hilft es, wenn man sechs Wochen auf ein „Pattern-Update“ warten muss und bis zu diesem Tag neue Viren unerkannt bleiben?

Die eingehende Prüfung von Datenströmen fordert selbstverständlich ihren Tribut. Die Performance der Gesamtlösung ist ein wesentliches Qualitätskriterium für die aufgebaute Firewall-Umgebung. Leidet die Geschwindigkeit der Datenübertragung spürbar, hat dies meist negative Auswirkungen auf die Akzeptanz der Umgebung durch die Benutzer und mindert der Produktivität. Ob eine E-Mail auf ihrem Weg zum Ziel-Server 142 Millisekunden oder 32,1 Sekunden benötigt, weil sie auf Computerviren hin untersucht wurde, ist für den Empfänger nicht zwangsläufig spürbar. Ob der Aufbau einer WWW-Seite jedoch 15 oder 45 Sekunden benötigt, ist für den Benutzer vor dem WWW-Browser durchaus von Bedeutung.

Für den Aufbau einer schlagkräftigen Umgebung zum Schutz gegen Viren und andere gefährdende Inhalt sind üblicherweise mehrere Produkte notwendig. Die „Alleskönner“ in diesem Bereich gibt es zwar ansatzweise, jedoch müssen auch diese Tool im einen oder anderen Anwendungsfall passen. Vor der Einführung eines solchen Produkts sollte allerdings zunächst die Frage im Mittelpunkt stehen, was und wovor man sich schützen möchte. Die Antwort auf die Frage nach dem geeigneten Produkt ergibt sich dann hieraus zwangsläufig. (kl)

Literatur

[1] Stefan Strobel, „Firewalls Einführung – Praxis – Produkte“, dPunkt Verlag Heidelberg, 2. Auflage 1999
[2] ActiveX and Java: The Next Virus Carriers, http://www.antivirus.com/download/whitepapers/activex.htm
[3] Finjan Software FAQ, http://www.finjan.com/support_FAQ.cfm

*** Christian Uwe Götz ist Diplominformatiker der Medizin und arbeitet als Berater für Netzwerksicherheitslösungen bei der Integraliscentaur in Heilbronn. E-Mail-Adresse: goetz@integraliscentaur.de**

HBCI und WAP als Plattformen für Bankgeschäfte

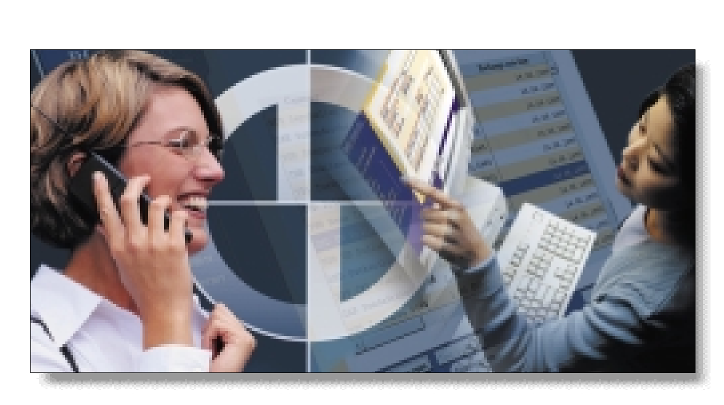
Mobile-Banking ohne Angst und Sorge

Christian Rademann*

Dienstleistungen, Handel, Bank- und jetzt auch Aktiengeschäfte – das Internet ist die ideale Plattform für den schnellen Vertrieb aller Waren und Informationen. Bestimmen das „virtuelle Kaufhaus“, Web-Auktionen oder der Verkauf von Bahn- und Flugtickets über das Internet schon seit langem unser virtuelles Leben, so werben nun auch Banken und Finanzdienstleister mit einem umfangreichen Service- und Dienstleistungsangebot im World Wide Web um ihre Kunden: Mittlerweile ist der elektronische Zugang zum eigenen Konto zum Standardprodukt avanciert. Depotabfrage, Aktienan- und -verkauf sind ebenfalls bei einem Großteil der Kreditinstitute abwickelbar. So kann der Kunde von daheim seine Bankgeschäfte tätigen, ohne länger an Schalteröffnungszeiten gebunden zu sein. Er braucht lediglich einen PC mit Internet-Anschluss und die entsprechende Banken-Software, um seine Kontostände abzufragen, Schecks anzufordern oder in Sekundenschnelle neue Wertpapierorders aufzugeben.

Zu Beginn des neuen Jahrtausends scheint sich jetzt ein neuer Trend am Markt durchzusetzen: Alles deutet darauf hin, dass sich die Verschmelzung der mobilen Erreichbarkeit des Handys mit den unendlichen Weiten des Internets nicht mehr aufhalten lässt. Mit der neuen WAP-(Wireless-Application-Protocol-)Technologie wird dem Bankkunden ein noch flexiblerer Kontozugangskanal eröffnet. Damit kann er schon bald – auf der CeBIT 2000 wurden die ersten Prototypen vorgestellt – neben PC, Call Center oder SB-Terminal seine täglichen Bank- und Aktiengeschäfte von jedem Ort der Welt, 24 Stunden, erledigen. WAP ist ein offener, globaler Standard für die Kommunikation mit mobilen Endgeräten und ermöglicht erstmals die direkte Kommunikation zwischen Mobiltelefon und PC. Laut jüngsten Studien werden in wenigen Jahren rund eine Milliarde Menschen mit dem Handy im Internet surfen und Flugtickets bestellen, Staumeldungen abfragen, Preisvergleiche anstellen und Aktienorder aufgeben. Dass dies keine Vision mehr ist, unterstreichen die vielversprechenden Wachstumsprognosen der Mobilfunkbetreiber und die stetig ansteigende Zahl von Handy-Besitzern: Ende 1999 stieg die Zahl der verkauften Handys auf 100 Millionen an, während „nur“ 80 Millionen Personalcomputer verkauft wurden. Darüber hinaus wird derzeit an der Verfügbarkeit neuer Standards wie etwa UTMS für einen noch schnelleren Zugang ins Internet gearbeitet. Gleichzeitig steigt die Nachfrage nach der mobilen Lösung bei Kaufhäusern, Nachrichtendiensten, privaten und öffentlichen Einrichtungen sowie Banken und Finanzdienstleistern stark an. Wo der Mobilität keine Grenzen mehr gesetzt sind, stellt sich dem kritischen Beobachter der zukünftigen Kommunikation mit der Bank eine Frage: Was bedeutet es, wenn persönliche Daten „online“ per PC oder Handy über das Internet verschickt werden?

Die Vorteile des mobilen WAP-Banking für den Endverbraucher liegen auf der Hand: Eine anwenderfreundliche, schnelle und zeitunabhängige Abwicklung der Bankgeschäfte über verschie-



Das WAP-Banking ermöglicht eine schnelle und zeitunabhängige Abwicklung der Bankgeschäfte über verschiedenste Medien

denste Medien bietet den Bankkunden geeigneten Service. So ist es etwa denkbar, dass ein Kunde über seinen PC Aktienorder aufgibt, deren Performance via Handy überwacht und in Echtzeit auf Kursveränderungen reagiert. Auch für die Finanzdienstleister verspricht das Geschäft über den neuen Vertriebskanal eine große Chance: Die Reichweite des Unternehmens vergrößert sich stark, potenzielle Neukunden können einfacher angesprochen werden. Gleichzeitig verringern sich interne Kosten für die Ablauforganisation, da Kundentransaktionen direkt ins System eingespeist und verarbeitet werden. Die manuelle Bearbeitung von Belegen oder Überweisungsträgern entfällt weitgehend. Darüber hinaus können sich die Bankberater wieder ihren Kernkompetenzen widmen und schaffen so sowohl für das Kreditinstitut als auch für den Bankkunden einen erheblichen Mehrwert: Kunde und Bank profitieren gleichermaßen von dem mobilen, zeitlich unbegrenzten Kommunikationsweg.

Der sichere Zugriff Da Banken und Mobilfunkindustrie höchste Sicherheitsanforderungen an die Umsetzung einer mobilen E-Banking-Lösung haben, sind die Software-Unternehmen gefragt, ihre Technologien ständig den neuen Herausforderungen und Bedürfnissen anzupassen. Die Münchner Datadesign versucht diesen Anforderungen mit ihrer modernen Multi-Channel-Banking-Plattform gerecht zu werden. Auf HBCI-(Homebanking-Computer-Interface-) Basis und unter Verwendung digitaler Signaturen sorgt die Plattform weit über die herkömmlichen PIN-/TAN-(Persönliche Identifikationsnummer/Transaktionsnummer-)Verfahren hinaus für den sicheren Informationsaustausch zwischen Kunde und Bank. In der Vergangenheit hat das Münchner Unternehmen mit mehreren Projekten bei namhaften Kreditinstituten bereits deutliche Akzente gesetzt.

Da die Transaktionsplattform der Datadesign schon jetzt unterschiedliche Vertriebskanäle von morgen – SB-Terminal, Call-Center, Internet-Fernseher oder auch Mobiltelefon – gleichermaßen erschließt, steht einer WAP-Anbindung bei den Kreditinstituten über die Multi-Channel-Banking-Plattform nichts im Wege. Denn alle Finanzdienstleister, die ihren Kunden heute oder in Zukunft sicheres Internet-Banking via HBCI ermöglichen, können diesen Zugang schnell und einfach WAP-fähig machen und somit innerhalb kürzester Zeit ihre Dienstleistungen über das Mobilfunknetz anbieten. Damit kann Handy-Banking ebenso sicher und komfortabel werden wie das Internet-Banking. Die Entwicklung neuer SIM-(Subscriber-Identity-Module-)Karten bietet darüber hinaus schon bald alle Features einer modernen Chipkarte inklusive Verschlüsselung und elektronischer Geldbörse.

Ob als reiner Dienstanbieter oder als Finanzportal, Banken und Sparkassen können mit der Datadesign-Lösung die WAP-Services im eigenen CI gestaltet und individuell angepasst werden. Die drahtlose Mobilität kann folglich als zusätzliche Werbeplattform genutzt werden und lässt die Bank Teil der mobilen Multimediagesellschaft werden. (kl)

*** Christian Rademann ist Manager Public Relations bei Datadesign.**

Datadesign
Tel. (089) 74 11 93 11
www.datadesign.de

Internet Solution Provider

Dienstleister Telefon	Angaben zur Firma		Webseiten-Gestaltung						Programmierungs-erfahrung								Erfahrung mit DB-Anbindung								Hosting-Angebote				Security-Dienstl.				Hosting von Application Services											E-Commerce-Dienstleist.					
	Zahl der festen Mitarbeiter	Zahl der Niederlassungen (BRD)	HTML	DHTML	XML	Audio	Video	Grafikdesign	XML	ASP	C/C++	Perl	PHP3	Java	JSCript	SQL	SQL-Server	Oracle	Informix	ODBC	Access	MySQL	Sybase	OODBMS	virtuelle NT-Server	Frontpage Extensions	SQL-Datenbank	Bandbreite d. Internet-Anbindung (MBit/s)	Security-Konzeption und Beratung	Digitale Zertifikate/Signaturen	Firewall-Einrichtung	VPN-Einrichtung	Web-Anwendungen	MS-Office	Terminal-Server	Lotus Domino	MS-Exchange	ERP-Anwendungen	E-Mail-Handling	Call-Center/CRM-Anwendungen	Online-Datenbanken	IP-Telefonie	Shop-Systeme	elektronische Zahlungssysteme	Electronic Billing	Shopping-Anwendungen	MS Site Server	EDI	XML
Aagon 0292/789200	18	1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●		●		●	2	●		●		●				●			●	●								
Adiscon 0800/2347266	6	2	●							●	●				●	●	●				●								●		●	●											●						
All Seitz 07231/584-0	550	3	●	●	●		●	●	●	●	●	●		●	●	●	●	●		●	●				●	●	●	4	●		●		●					●		●			●	●		●	●	●	●
Aspia 06105/25474	5	1	●	●	●			●	●		●	●		●	●	●	●	●	●	●	●		●	●																									●
Ewald Baumann 0651/9930030			●	●		●	●	●		●	●	●		●	●	●	●			●	●	●			●								●						●				●			●			
Beans Industry 0881/98994-38	72	5	●		●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●			●	●			●			●		●	●	●	●		●	●	●	●	●	●	●
Berens/Partner 0211/39004-0	120	4	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●		●	●	●	●	●	●		●	2	●	●	●	●	●						●	●	●		●	●	●	●	●	●	●
Binworx 06221/89540-0	5	2	●	●	●			●	●	●	●				●	●	●	●	●	●	●		●		●	●	●						●					●	●		●			●		●	●	●	●
Business Online 0621/126940	40	6	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●		●	●	●	●		●	●	●	●	●										●	●	●	●			●
Cats 0361/2246-0	10	2	●					●			●	●		●		●	●	●		●		●			●	●	●	2	●		●	●	●		●				●	●	●		●						
Comline App. Serv. 0231/97575-130	95	2							●	●	●			●	●	●	●	●	●										●		●		●							●						●			●
Comline Dokument Mgmt. Serv. 0231/97575-130	95	2	●	●	●			●	●		●	●		●	●	●	●	●	●	●	●				●		●		●	●	●	●	●			●			●		●		●			●			
Conit 06022/262-082	5	1	●		●				●		●	●	●	●		●	●	●	●	●		●	●						●		●																		
Consultix 0421/33388-0	7	1	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●		●			●		●	●	●		●	●	●	●	●		●		●		●		●		●	●		●	●		●
CSC 0251/23004-0	55	2	●	●	●				●		●			●		●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●			●	●		●	●	●	●	●	●		●	●
Deutsche Post Com 02102/479-121	90	2																											●	●			●			●								●	●			●	
Deutsche Telekom 0800/8353732																													●	●	●	●																	
Digalog 030/46702-0	22										●					●	●		●	●							●								●						●								
E.Comp 06151/88008-0	75	3	●					●					●					●							●	●	●		●		●	●	●																
Easynet 089/545831-0	20	2									●			●			●	●	●	●	●							2,34	●		●	●							●			●					●		
Elmedia 04102/8036-0	6	1	●	●	●	●	●	●	●		●			●	●	●	●	●	●	●	●	●	●		●		●						●			●							●	●		●			●
ESC 0345/55844-0	15	1	●		●			●	●		●	●	●	●	●	●				●	●	●	●			●	●		●		●	●	●						●		●		●			●			●
Eurolink Service 0221/4992076	6	1	●	●		●	●	●				●	●		●	●	●			●	●	●				●	●	2	●		●		●								●		●	●		●			
Europop 0211/386630	30								●	●	●	●	●	●	●	●	●	●		●					●	●	●	2	●	●	●	●	●	●	●	●	●		●		●	●	●			●			
Fun 0721/96448-164	50	2																											●	●		●												●					
GFT Systems 03677/6429-0	42	2	●	●	●					●	●			●	●	●	●	●	●	●	●		●	●					●																	●			●
Giganet 0611/973750	4	1	●	●	●				●	●				●	●	●	●	●		●	●		●						●	●																			●
Gronen 0221/9321-000	6	1	●	●	●	●	●	●	●		●	●	●			●						●					●	210															●						
Global Telesystems 0800/1040-800	400	12																							●								●						●										

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

Internet Solution Provider

Dienstleister Telefon	Angaben zur Firma		Webseiten-Gestaltung						Programmierungs-erfahrung								Erfahrung mit DB-Anbindung								Hosting-Angebote				Security-Dienstl.				Hosting von Application Services											E-Commerce-Dienstleist.					
	Zahl der festen Mitarbeiter	Zahl der Niederlassungen (BRD)	HTML	DHTML	XML	Audio	Video	Grafikdesign	XML	ASP	C/C++	Perl	PHP3	Java	JScript	SQL	SQL-Server	Oracle	Informix	ODBC	Access	MySQL	Sybase	OODBMS	virtuelle NT-Server	Frontpage Extensions	SQL-Datenbank	Bandbreite d. Internet-Anbindung (MBit/s)	Security-Konzeption und Beratung	Digitale Zertifikate/Signaturen	Firewall-Einrichtung	VPN-Einrichtung	Web-Anwendungen	MS-Office	Terminal-Server	Lotus Domino	MS-Exchange	ERP-Anwendungen	E-Mail-Handling	Call-Center/CRM-Anwendungen	Online-Datenbanken	IP-Telefonie	Shop-Systeme	elektronische Zahlungssysteme	Electronic Billing	Shopping-Anwendungen	MS Site Server	EDI	XML
HEC 0421/20750-0	54	1	●	●	●				●	●	●			●	●	●	●	●	●	●	●		●	●					●															●	●	●	●	●	●
Heureka 07152/939310	7	1	●	●	●			●	●		●	●		●	●	●	●	●		●	●	●		●			●	bel.	●	●		●	●						●	●	●		●	●		●			●
Hut 05121/17937-0	12	2							●	●	●	●	●	●		●	●	●		●	●	●											●					●			●		●			●			●
Hyperspace 05171/591900	4	1	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	2-115	●	●	●	●	●	●	●		●	●	●		●	●	●	●	●	●			●
Information Arch. 0941/585660	20	1	●	●	●	●	●	●	●	●	●			●	●	●	●	●		●	●	●		●					●					●	●	●	●		●	●	●	●	●	●		●	●		●
IAP 040/306803-0	8	2	●	●				●			●	●		●			●			●	●	●		●	●	●		2			●		●						●		●		●			●			
IAS 0721/96416-0	100	1	●		●			●	●	●	●	●		●	●	●	●	●	●	●			●				●		●	●	●	●	●				●	●			●			●	●	●		●	
IBH Prof. Dr. Horn 0351/4777720	10	1																											●		●	●																	
IBS 0631/36696-47		2	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		●	●	●	●	●	●	●	●	●	●	●		●		●	●	●	●	●	●	●
Incas 02152/1435-0	15	1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●		●	●	●	2x2	●		●	●	●	●		●	●		●	●	●	●	●			●		●	●
Infoserv 07422/9549-11	13	1	●	●							●			●	●					●								2					●			●			●		●		●			●			
Inosoft 06421/581500	32	1	●	●	●				●	●				●	●	●	●			●					●		●	2x2	●	●	●		●	●	●		●		●		●		●	●		●	●		●
INS 02305/101-0	30	1	●	●		●					●	●		●	●	●	●		●	●	●	●			●		●	2x34	●		●	●	●						●				●			●			
Intec Consulting 07361/974141	70	2	●	●	●			●	●	●	●				●	●	●			●	●	●							●				●	●	●		●				●					●	●		●
Internetwork 0611/16657-0		1	●	●	●			●	●		●	●		●	●	●	●	●	●	●	●		●					2	●				●										●	●	●	●			●
Intradat 069/97405703	20	2									●					●																														●			
Intraware 0661/9642211	110	6	●	●				●	●		●	●		●	●	●		●		●	●		●													●		●	●		●		●	●		●			●
ISA Tools 0711/2276915	40	1	●	●	●		●	●	●	●	●	●		●		●	●	●	●	●	●			●		●			●	●	●		●										●	●	●	●		●	●
Isoft 030/723922-49	35		●		●			●	●		●	●	●	●	●	●	●	●	●	●		●	●						●		●	●	●						●		●		●	●	●	●		●	●
ISR Netcom 0231/737848	4	2	●	●	●	●	●	●	●			●		●	●	●	●			●	●	●			●		●	10	●		●	●	●						●		●			●	●	●			●
IT Protect 02332/7596-00	4	2	●	●	●			●	●	●	●	●	●	●	●	●	●	●		●		●			●		●	4	●	●	●	●	●						●		●	●	●	●	●	●			●
ITB 0571/8709-17	14	1	●	●	●			●	●	●	●	●	●	●	●	●	●			●	●	●			●	●	●	8	●	●	●	●	●						●		●		●			●			●
ITZ 0221/49707-35	70	7	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●		●	●	●	2		●	●		●	●		●	●		●		●		●	●		●			●
Ixnet 06251/9330-0																												100	●	●	●	●																	
Inf.verarb. M. Jeschak 02332/82987	3	1	●	●	●				●		●			●	●	●	●			●			●								●	●	●						●										
INW 040/63918824	10	1	●	●	●			●		●	●		●	●	●	●	●		●	●	●	●	●						●	●	●	●											●			●			
KDT 0202/495-320	30					●	●					●	●			●				●		●			●	●	●	18	●	●	●	●	●				●		●		●	●	●	●	●	●			
Kompakt Software 06894/103320	4	1	●		●			●	●	●	●			●	●	●	●			●	●				●		●						●								●		●			●		●	●
Krauss Systeme 0511/319274	6	1	●		●	●	●	●	●	●		●		●	●	●	●	●		●	●				●	●	●	155-622	●	●	●	●	●		●	●							●	●		●			●
Login S+C 0228/97859-0	20		●					●			●	●		●	●	●	●		●	●	●		●		●	●	●		●		●			●	●		●		●		●								

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

Internet Solution Provider

Dienstleister Telefon	Angaben zur Firma		Webseiten-Gestaltung						Programmierungs-erfahrung								Erfahrung mit DB-Anbindung								Hosting-Angebote				Security-Dienstl.				Hosting von Application Services											E-Commerce-Dienstleist.					
	Zahl der festen Mitarbeiter	Zahl der Niederlassungen (BRD)	HTML	DHTML	XML	Audio	Video	Grafikdesign	XML	ASP	C/C++	Perl	PHP3	Java	JSCript	SQL	SQL-Server	Oracle	Informix	ODBC	Access	MySQL	Sybase	OODBMS	virtuelle NT-Server	Frontpage Extensions	SQL-Datenbank	Bandbreite d. Internet-Anbindung (MBit/s)	Security-Konzeption und Beratung	Digitale Zertifikate/Signaturen	Firewall-Einrichtung	VPN-Einrichtung	Web-Anwendungen	MS-Office	Terminal-Server	Lotus Domino	MS-Exchange	ERP-Anwendungen	E-Mail-Handling	Call-Center/CRM-Anwendungen	Online-Datenbanken	IP-Telefonie	Shop-Systeme	elektronische Zahlungssysteme	Electronic Billing	Shopping-Anwendungen	MS Site Server	EDI	XML
Lynet 0451/6131-0	10	3	●					●			●	●	●	●	●	●		●	●	●	●	●				●	●		●	●	●	●	●						●		●	●	●			●			
Magic Software 089/96273-0	770	2	●		●	●	●	●	●					●			●	●	●	●			●						●	●	●	●	●							●	●		●	●	●	●		●	●
M@kom 02234/943231	4	1	●				●	●																																			●						
MConsult 089/44229-0	15	1	●	●	●			●	●	●	●	●			●	●	●	●	●	●	●		●	●	●	●	●	10	●	●	●	●	●	●			●		●		●						●		●
Mediaways 05241/80-2223	130	3							●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	155	●	●	●	●	●	●	●	●	●	●	●	●	●	●							
Motiva 09131/7777-10	25	1	●		●			●	●	●	●	●	●	●	●	●	●			●	●	●			●	●	●	2	●			●	●	●	●		●		●								●		
Müller-Knoche 0911/93488-0	20	1	●	●				●	●			●		●															●		●	●											●			●			
MS Com 040/25490054	5	1								●	●					●	●	●		●	●					●	●		●	●	●	●		●			●		●		●						●		
Net. 0711/97689-21	3	1	●					●			●	●	●	●	●	●						●				●	●	2	●		●	●	●						●		●		●			●			
Net 2000 0211/436270	18	1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●							●	●	●	●	●			●			●	●			●			●			●
Netuse 0431/3864500	60	1	●	●	●			●	●		●	●	●		●	●		●	●			●			●		●	3x2	●	●	●	●	●						●		●	●	●			●			●
Network Domains 08021/8879-0	5	1																																															
Netzland 09122/2050	10	1	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●		●	●	●			●		●	34	●	●	●	●	●	●		●	●		●	●	●		●	●	●	●	●		
NT-Kommunikations-system 02064/46900	6	1	●	●		●	●	●		●	●		●	●	●	●	●			●	●	●			●	●	●	4	●	●	●		●	●			●		●		●		●	●		●	●		
Octet 05401/8280-0	5								●		●	●	●	●	●	●		●		●	●	●		●																						●			●
On 0221/9320152	5	1	●	●				●				●		●	●	●			●				●						●				●										●	●	●	●		●	
Optimum 07146/871060	22	2	●		●				●		●	●		●	●	●	●	●	●	●	●			●																									
Origin 040/7886434	1100	13	●		●				●	●	●	●		●	●	●	●	●	●	●	●	●	●	●			●		●	●	●	●	●			●	●	●	●	●	●		●	●	●	●	●	●	●
P + I 0611/7147-228	220	9																																				●											
PC-Studio 0212/26799-0	40	1	●	●	●			●	●	●	●	●		●		●	●			●	●	●			●	●	●	34	●	●	●	●	●	●	●		●	●	●	●	●		●	●	●	●	●	●	●
PDV-Systeme 03528/4803-0	22	1	●					●									●	●		●	●	●				●	●	2	●		●	●	●	●	●		●		●			●							
Pica 089/25551-0	35	1	●	●	●				●	●	●	●		●	●	●	●	●		●	●				●		●	256 kB			●		●						●										
Piwinger + Lau 0261/30412-0	25	2	●	●	●			●	●	●	●	●		●	●	●	●	●			●				●	●	●	1,5	●		●	●	●	●	●		●		●		●		●			●	●	●	●

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info ▶

Internet Solution Provider

Dienstleister Telefon	Angaben zur Firma		Webseiten-Gestaltung						Programmierungs-erfahrung								Erfahrung mit DB-Anbindung								Hosting-Angebote				Security-Dienstl.				Hosting von Application Services											E-Commerce-Dienstleist.					
	Zahl der festen Mitarbeiter	Zahl der Niederlassungen (BRD)	HTML	DHTML	XML	Audio	Video	Grafikdesign	XML	ASP	C/C++	Perl	PHP3	Java	JScript	SQL	SQL-Server	Oracle	Informix	ODBC	Access	MySQL	Sybase	OODBMS	virtuelle NT-Server	Frontpage Extensions	SQL-Datenbank	Bandbreite d. Internet-Anbindung (MBit/s)	Security-Konzeption und Beratung	Digitale Zertifikate/Signaturen	Firewall-Einrichtung	VPN-Einrichtung	Web-Anwendungen	MS-Office	Terminal-Server	Lotus Domino	MS-Exchange	ERP-Anwendungen	E-Mail-Handling	Call-Center/CRM-Anwendungen	Online-Datenbanken	IP-Telefonie	Shop-Systeme	elektronische Zahlungssysteme	Electronic Billing	Shopping-Anwendungen	MS Site Server	EDI	XML
PK Software 08121/912014	4	1	●	●	●			●			●	●				●				●	●	●			●	●	●			●			●						●		●		●			●			
Prahm 0721/558995	3	2	●	●	●			●	●		●			●		●	●				●					●	●						●	●					●										●
PSP Net 06430/2222	30	1								●		●		●		●	●			●	●			●	●	●	●	10	●	●	●	●	●		●				●		●		●						
Richtmann + Eder 089/35487-126	70	2	●	●	●			●	●	●	●	●	●	●	●	●	●	●		●	●	●						2	●	●	●	●	●						●		●		●			●			
Rietschel 0700/888888-30	18	3	●	●	●	●	●	●	●		●			●	●	●	●			●	●		●		●			155	●	●	●	●	●		●	●			●		●		●			●		●	●
Ritz Soft-Media 089/74016993			●	●	●	●	●	●	●		●			●	●	●		●	●	●	●	●	●	●	●		●	144	●			●	●				●	●	●	●	●	●	●	●		●		●	●
EDV-Ber. Schulze 0511/972980	5		●			●	●	●		●				●	●	●	●			●	●				●	●	●	4					●	●			●		●		●		●			●	●		
Securenet 02054/123-115																													●	●	●	●																	
Secorvo 0721/6105-452		1																											●	●	●	●																	
Seeburger 07252/9358-132	240	6	●	●	●			●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●									●			●					●		●			●		●	●
SK-Computerdienst 0211/36975-34	25		●														●				●					●			●	●			●	●	●		●						●						
SHE 0621/5200-229	110	3	●	●	●				●	●	●	●	●	●	●	●	●	●		●	●	●			●	●		10	●	●	●	●	●			●			●		●		●			●			
Signsoft 0351/89453-12	15	1	●	●	●			●	●		●	●		●	●	●	●	●	●	●	●	●	●	●					●														●	●		●			
Software Symbiose 0921/761260	7	1	●	●					●	●	●	●	●	●	●	●	●			●	●	●			●	●	●	2	●		●	●	●				●		●		●	●	●			●			
Tiscon 0731/95448-100	190	5	●		●				●	●	●	●	●	●	●	●	●	●	●	●	●	●		●			●		●		●		●	●		●		●		●		●		●					
Topologix 040/352253	15	1									●	●		●		●	●	●	●				●						●		●	●																	
Traicen 06251/4876	15	1								●	●						●	●		●	●			●					●	●	●	●																	
Trisoft 0511/94294-0	2	1	●			●	●	●			●	●		●	●	●	●				●						●	34	●	●	●	●	●						●		●		●	●	●	●		●	
Unirent 04192/879666	4	2	●		●			●	●	●	●				●	●	●			●	●				●	●	●		●	●	●		●				●		●		●			●	●	●		●	
Vectorsoft 06104/660-100			●	●				●			●	●		●	●	●	●									●							●						●		●		●			●	●		
VSS 02203/24194	6		●	●	●					●	●			●	●	●	●	●	●	●		●							●		●	●		●	●				●		●		●	●	●	●			
Web Data Center 07171/187-212	30	2										●	●	●			●				●							2	●	●	●																		
Websale 09127/9521-0	12	1	●	●	●	●	●	●	●		●	●	●	●	●		●					●			●			124		●			●						●				●	●	●	●			●
Weilgut 07243/5466-0	32	1	●								●			●	●		●				●								●							●			●	●	●	●							
Werum 04131/8900-0	160	3	●	●				●	●		●	●		●	●	●	●	●	●	●	●	●	●	●			●	2	●	●	●	●	●								●			●		●		●	●
What's up 089/61437-0	31	1															●	●	●	●	●	●	●		●			34	●			●	●			●			●	●	●	●	●	●	●	●		●	●
Wolff 05222/959643	1	1	●					●												●							●	a. A.	●														●			●			
WWW-Service 0800/9994636	40	1	●	●				●				●	●		●	●						●			●	●													●		●		●			●			
Zet Net 08031/213-250	7	1	●	●	●	●	●	●		●		●	●		●	●	●			●	●	●			●	●	●	2	●		●		●						●	●	●	●	●	●		●			

Weitere Informationen und Weblinks finden Sie unter www.win2000mag.de/info

Informationen schnell per Fax oder Internet

Inserenten

Inserent	Seite	Kennz.
AddOn Systemhaus	15	6
APC	27	11
asb Systemhaus	59	22
AVM Computersysteme	63	24
CommVault Systems	31	13
CommVault Systems	99	31
Computer Competence	94	Seminarführer
ComputerLinks	94	Seminarführer
Conditio	94	Seminarführer
DITEC	95	Seminarführer
Dr Materna	3	2
DV-Job.de	79	30
DV-Markt	70	25
EDC Business Computing	94	Seminarführer
Eicon Technology Diehl	13	5
Enterprise International	7	4

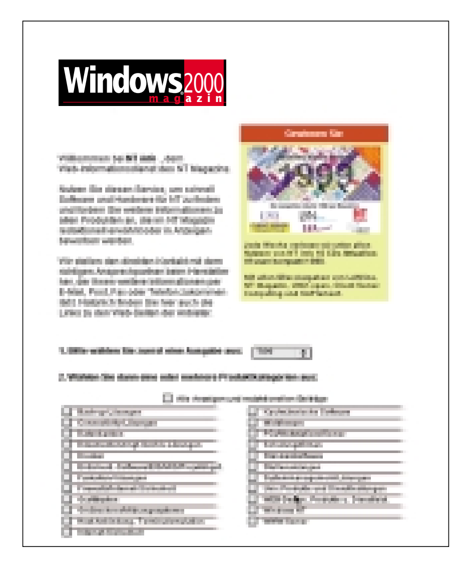
Inserent	Seite	Kennz.
Ferrari Electronic	19	8
Fujitsu	2	1
Globalsoft Solutions	57	21
Hewlett-Packard	37	14
Hilf!	95	Seminarführer
ISP*D Akademie	95	Seminarführer
Itellium System & Services	55	20
Kölsch & Altmann	94	Seminarführer
LANWORKS	95	Seminarführer
LANWORKS	100	32
Login S&C	95	Seminarführer
MGE USV-Systeme	25	10
MuTek Solutions	17	7
NetSupport	75	28
PCI Software	39	15
Peacock	61	23

Inserent	Seite	Kennz.
PSP Net	49	19
Retarus Network Services	71	26
Softmatic	95	Seminarführer
Sony	23	9
Sunbelt Software Distribution	29	12
Sydios it solutions	47	18
Systems Group	43	17
The Bristol Group	95	Seminarführer
Trefz & Partner	5	3
Trefz & Partner	95	Seminarführer
Unilab Computersysteme	73	27
Xnet Communications	41	16

Einhefter

Network Appliance

Recherche im WEB



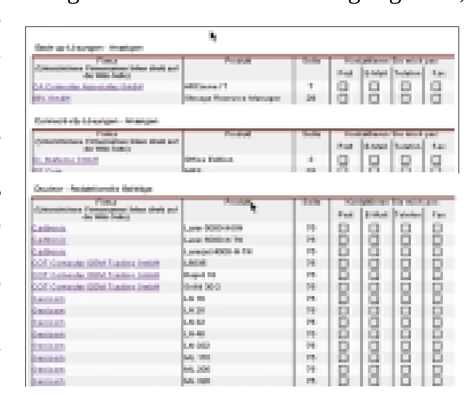
Der Web-Kennzifferndienst des Windows 2000 Magazins macht die gezielte Suche im WWW so komfortabel und schnell wie nie zuvor. Dieses Tool funktioniert im Prinzip wie das Leser-Info-Fax, das den Lesern ja seit Jahren vertraut ist, allerdings mit erheblich erweiterten Möglichkeiten und allen Vorteilen des World Wide Web: Sie suchen in unserer Online-Datenbank die für Sie interessanten Produkte. Dann entscheiden Sie, in welcher Form Sie kontaktiert werden möchten. Wir leiten Ihre Anfrage an den Ansprechpartner weiter, der Sie dann auf dem von Ihnen gewünschten Weg kontaktiert. Und so funktioniert der Webkennzifferndienst: Unter

http://www.win2000mag.de/info

wählen Sie zunächst aus, in welcher Ausgabe des Windows 2000 Magazins Sie recherchieren möchten. Dann wählen Sie eine oder mehrere Produktkategorien aus. Alternativ können sie, falls Sie schon genau wissen, wofür Sie sich interessieren, direkt den Namen des Anbieters oder die Kennziffer der Anzeige eingeben. Zusätzlich steht Ihnen noch die Option “Alle Anzeigen und redaktionellen Beiträge” zur Verfügung. Drücken Sie die Schaltfläche “Weiter”, um Ihre Abfrage zu starten.

Das System stellt nun eine Liste aller Inserenten und redaktionellen Beiträge zusammen, die Ihren Suchkriterien entsprechen. Wenn die Firma eine eigene Website besitzt, dann ist der Firmenname in der linken Spalte mit einem Hyperlink unterlegt. Damit kommen Sie direkt auf die Web-Seiten des Anbieters. Wichtig für Ihre Info-Anforderung sind die letzten vier Spalten. Hier können Sie bei jeder Firma ankreuzen, ob Sie weitere Informationen per E-Mail, Post, Fax oder Telefon erhalten möchten. Selbstverständlich können Sie hier mehr als eine Firma ankreuzen. Auf diese Weise können Sie ohne zusätzlichen Aufwand gleich mehrere Anfragen generieren. Bei der erstmaligen Benutzung des Webkennzifferndiensts drücken Sie jetzt einfach den “Weiter”-Button und gelangen damit zur Eingabemaske für Ihre Kontaktinformationen. Noch schneller geht es, wenn Sie das System schon einmal benutzt haben. Dann reicht die Eingabe Ihrer E-Mail-Adresse aus, und ihre Daten werden automatisch ergänzt.

Wenn Sie jetzt “Weiter” drücken, gelangen Sie auf eine Bestätigungsseite,



und das System generiert für jeden der von Ihnen angekreuzten Anbieter eine Anfrage, die per E-Mail an den zuständigen Ansprechpartner verschickt wird. Dieser setzt sich mit Ihnen auf dem von Ihnen gewünschten Weg in Verbindung. Auf der Bestätigungsseite finden Sie außerdem eine kleine Online-Umfrage, deren Ergebnisse uns dabei helfen, das Windows 2000 Magazin auch weiterhin mit den richtigen Informationen für Sie zu füllen.

INFOFAX

-> www.win2000mag.de oder 089/45616-300

Windows 2000 Magazin 7/2000

So erhalten Sie weitere Informationen zu den in dieser Ausgabe veröffentlichten Anzeigen.

Info-Fax ◀ # 023 ▶ www.win2000mag.de/info Tragen Sie die entsprechende Kennziffer unter **www.win2000mag.de/info** an der vorgesehenen Stelle ein und Sie gelangen direkt und ohne Umwege zu Ihren gewünschten Zusatzinformationen.

Info-Fax ◀ # 023 ▶ www.win2000mag.de/info Selbstverständlich haben Sie nach wie vor die Möglichkeit, weitere Anzeigen-Produkt-Infos mit dem unten stehenden Faxformular abzurufen. Einfach ausfüllen und an die Fax-Nummer **0 86 21/97 99 60** faxen. Zum schnellen Überblick haben wir alle inserierenden Firmen auf der gegenüberliegenden Seite aufgelistet.

Meine Anschrift lautet:

Firma . . . .

Abteilung . . . .

Vorname/Name . . . .

Straße/Nummer . . . .

PLZ/Ort . . . .

Telefon . . . .

Fax . . . .

Ich möchte Informationsmaterial zu Produkten und Anzeigen mit folgender Kennziffer:

1.	2.	3.
4.	5.	6.
7.	8.	9.
10.	11.	12.

Mein Unternehmen beschäftigt:

- ❒ 1 bis 19 Mitarbeiter
- ❒ 20 bis 49 Mitarbeiter
- ❒ 50 bis 99 Mitarbeiter
- ❒ 100 bis 249 Mitarbeiter
- ❒ 250 bis 499 Mitarbeiter
- ❒ 500 bis 999 Mitarbeiter
- ❒ über 1000 Mitarbeiter

Meine Funktion im Unternehmen:

- ❒ Spezialist
- ❒ Einkauf
- ❒ Gruppen-/Abteilungsleiter
- ❒ Unternehmensleitung

Ich interessiere mich für folgende Produkte und Themen:

Software-Infrastruktur

- ❒ Betriebssysteme
- ❒ Entwicklungswerkzeuge
- ❒ Systems Management
- ❒ Electronic Commerce
- ❒ Groupware
- ❒ Middleware
- ❒ Anwendungssoftware
- ❒ andere . . . .

Datenmanagement

- ❒ Relationale Datenbanken
- ❒ OO-Datenbanken
- ❒ Storage und Backup
- ❒ Data Warehousing
- ❒ Data Mining/OLAP
- ❒ Reporting
- ❒ Dokumentenmanagement
- ❒ andere . . . .

Netzwerkintegration

- ❒ Netzwerkkomponenten
- ❒ Computer/Telephonie-Integration
- ❒ Netzwerkmanagement
- ❒ Internet/Intranet
- ❒ Netzwerk-Security
- ❒ Remote Access-Lösungen
- ❒ Video-Conferencing
- ❒ ISDN
- ❒ Host-Anbindung
- ❒ andere . . . .

Hardware

- ❒ Server-Systeme
- ❒ Workstations
- ❒ PCs
- ❒ Speichertechnologien
- ❒ NCs
- ❒ Terminals
- ❒ Drucker
- ❒ Monitore
- ❒ PC-Komponenten
- ❒ Peripheriegeräte
- ❒ andere . . . .

Ich plane in den nächsten 12 Monaten Investitionen in

- ❒ Software
- ❒ Datenmanagement
- ❒ Netzwerk und Kommunikation
- ❒ Hardware

Damit Hersteller und Anbieter von Produkten, für die ich mich interessiere, meine Kennziffernanfragen so gezielt wie möglich beantworten können, bin ich damit einverstanden, dass diese Daten elektronisch gespeichert und weitergegeben werden.

Ort, Datum Unterschrift

INFO PER FAX ODER INTERNET

Lab-Report



- *Backup-Software für Firmennetzwerke im Vergleich*
- *Performance-Vergleich: Windows NT 4.0 kontra Windows 2000 Professional*
- *Marktübersicht: Backup-Hardware mit Windows-NT/Windows-2000-Support*

Know-how für NT und Windows 2000



- *Peripherie: So wird der Windows-2000-PC zum Videostudio*
- *Grundlagen: So funktionieren die Dienste in Windows NT und Windows 2000*
- *Flexible Festplattenverwaltung durch dynamische Datenträger*

Dokumenten-management und Archivierung

- *Scan-Lösungen für den High-end-Einsatz*
- *Hierarchisches Storage Management mit dem Remote Storage Service von Windows 2000*
- *Marktübersicht: Archivierungssysteme für Windows NT und Windows 2000*

Themenänderung aus aktuellem Anlass vorbehalten

Die nächste Ausgabe von Windows 2000 Magazin erscheint am 4. August 2000

Impressum

Herausgeber: Eduard Heilmayr
Chefredaktion: Frank-Martin Binder (fbi), verantwortlich für den redaktionellen Inhalt (-123)
Redaktion: Otto Klusch (kl) (-220), Wolfgang Patelay (pa) (-227)
Redaktionsassistenz: Nicky Amann (-221)
Autoren dieser Ausgabe: Ulf Altner, Bob Chronister, J. Simon Hancock, Mark Minasi, Tony Redmond, John Ruley, Larry Seltzer, R. Franklin Smith, Benjamin Stein, Tanja Stephani, Leo Strassmann, Clemens Thielecke, Uwe Thiemann
Übersetzungen: Keven Sarlo
Feste freie Mitarbeiter: Benjamin Stein, Markus Bernauer (Lab), Albert Kern (Lab)

So erreichen Sie die Redaktion: Bretonischer Ring 13, 85630 Grasbrunn, Tel. (089) 45616-221, Telefax (089) 45616-300

Manuskripteinsendungen: Manuskripte werden gerne von der Redaktion angenommen. Sie müssen frei sein von Rechten Dritter. Sollten sie auch an anderer Stelle zur Veröffentlichung oder gewerblichen Nutzung angeboten worden sein, muß das angegeben werden. Mit der Einsendung gibt der Verfasser die Zustimmung zum Abdruck in den von der AWi Aktuelles Wissen Verlag GmbH herausgegebenen Publikationen. Honorare nach Vereinbarung. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen.

Titelbild- und Layout-Gestaltung: Ilona Kocksch
DTP-Produktion: Hans Fischer, Michael Szonell, Edmund Krause (Leitung)

Anzeigenleitung: Corinna Weiss, Tel. (0 89) 4 56 16-113 – verantwortlich für Anzeigen
Anzeigenverwaltung: Gabi Fischböck, Tel. (0 89) 4 56 16-262
Anzeigendisposition: Sandra Pablitschko, Tel. (0 89) 4 56 16-108

Anzeigenpreise: Es gilt die Preisliste Nr. 8 vom 1.1.2000
So erreichen Sie die Anzeigenabteilung: Tel. (089) 45616-113, Telefax (089) 45616-250

Vertrieb Handel: MZV, Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Straße 5, Postfach 1123, 85386 Eching, Tel. (089) 31906-0

Erscheinungsweise: monatlich (zwölf Ausgaben im Jahr)

Zahlungsmöglichkeiten für Abonnenten: Bayerische Vereinsbank München, BLZ 700 202 70, Konto: 32 248 594; Postgiro München, BLZ 70010080, Konto: 537040-801

Bezugspreise: Das Einzelheft „Windows 2000 Magazin" kostet DM 9,00. Der Abonnement-Preis beträgt im Inland DM 96,- pro Jahr für 12 Ausgaben. Darin enthalten sind die gesetzliche Mehrwertsteuer und Zustellgebühren. Der Abonnement-Preis erhöht sich auf DM 122,- für die Zustellung im Ausland.

Vertrieb: Abonnement-Bestellungen und Adressänderungen richten Sie bitte an: Edith Winklmaier, Herzog-Otto-Straße 42, 83308 Trostberg, Tel. 0 86 21/64 58 41, Fax 0 86 21/6 27 86

Druck: Hudack Druck GmbH, Dieselstraße 22, 85748 Garching-Hochbrück

Sonderdruckservice: Alle in dieser Ausgabe erschienenen Beiträge sind in Form von Sonderdrucken erhältlich. Anfragen richten Sie bitte an Alfred Neudert, Tel. 089/45616-146 oder Edmund Krause, Tel. (0 89) 4 56 16-240, Fax 089/45616-250.

Verlagsleitung Windows 2000 Magazin: Frank-Martin Binder

Anzeigenverkaufsleitung AWi Verlag: Cornelia Jacobi, Tel. 089/71940003

Geschäftsführer: Eduard Heilmayr

Anschrift des Verlages: AWi NT Magazin Verlagsgesellschaft mbH, Bretonischer Ring 13, 85630 Grasbrunn

www.win2000mag.de

ISSN 1438-4353

Diese Zeitschrift wird mit chlorfreiem Papier hergestellt.

Windows 2000 ist ein registriertes Warenzeichen von Microsoft Corporation.